PK3

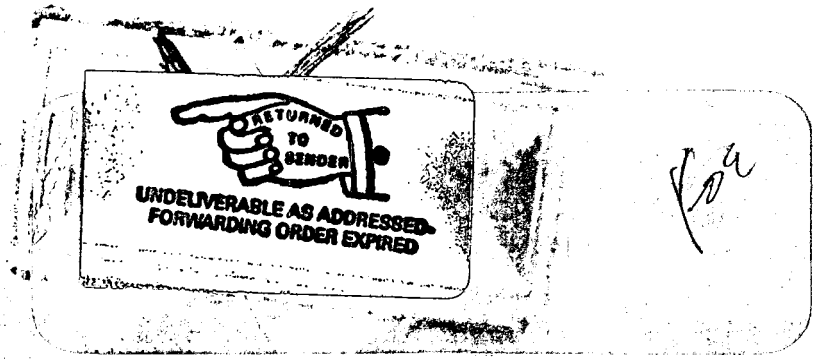
Organization_____ Bldg./Room_____

U. S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
WASHINGTON, DC 20231
IF UNDELIVERABLE RETURN IN TEN DAYS

OFFICIAL BUSINESS

AN EQUAL OPPORTUNITY EMPL

WASHINGTON OCT 07 03 DC
U.S. OFFICIAL MAIL
PENALTY FOR PRIVATE USE $300
PB METER 7249720
455
U.S. POSTAGE



for

Return to Sender
THIS COMPANY MOVED
OVER TWO YEARS AGO.
DON'T KNOW WERE
NO SUCH PERSON
CO. AT THIS ADDRES

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/600,364	07/14/2000	THOMAS ZELLERHOFF	P001334	2637

7590 10/07/2003

HILL STEADMAN & SIMPSON
85TH FLOOR SEARS TOWER
CHICAGO, IL 60606

EXAMINER	
NGUYEN, VAN KIM T	

ART UNIT	PAPER NUMBER
2661	7

DATE MAILED: 10/07/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

US005768271A

United States Patent [19]

Seid et al.

[11] Patent Number: 5,768,271

[45] Date of Patent: Jun. 16, 1998

[54] **VIRTUAL PRIVATE NETWORK**

[75] Inventors: **Howard A. Seid**, Fairfax, Va.; **Albert Lespagnol**, Le Bretonneux, France

[73] Assignee: **Alcatel Data Networks Inc.**, Ashburn, Va.

[21] Appl. No.: **632,168**

[22] Filed: **Apr. 12, 1996**

[51] **Int. Cl.**[6] **H04L 12/56**

[52] **U.S. Cl.** **370/389**; 370/397

[58] **Field of Search** 370/389, 390, 370/392, 393, 394, 395, 396-400, 352, 356, 357, 355, 402, 409, 428

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,348,554	9/1982	Asmuth	370/96
4,823,338	4/1989	Chan et al.	370/85.2
5,274,643	12/1993	Fisk	370/94.1
5,337,307	8/1994	Sato et al.	370/60
5,357,564	10/1994	Gupta et al.	379/188
5,394,402	2/1995	Ross	370/94.1
5,432,783	7/1995	Ahmed et al.	370/60.1
5,432,785	7/1995	Ahmed et al.	370/60.1
5,436,909	7/1995	Dev et al.	371/20.1
5,440,547	8/1995	Easki et al.	370/60
5,442,637	8/1995	Nguyen	370/94.1
5,446,734	8/1995	Goldstein	370/60.1
5,452,293	9/1995	Wilkinson et al.	370/395
5,477,536	12/1995	Picard	370/60

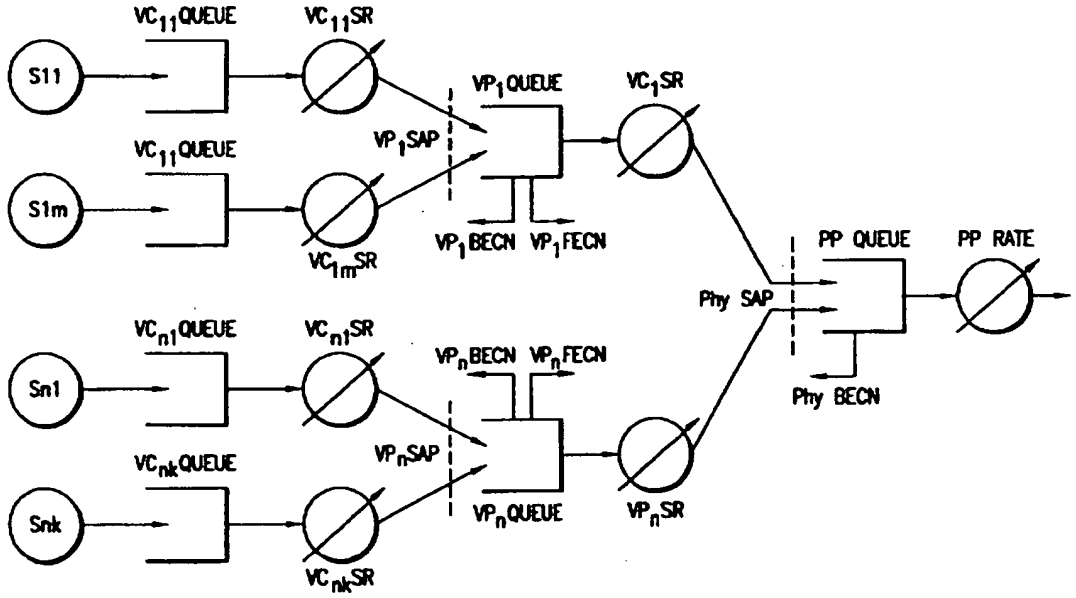
Primary Examiner—Dang Ton

Attorney, Agent, or Firm—Ware, Fressola Van Der Sluys & Adolphson LLP

[57] **ABSTRACT**

In a packet switching (packet-based) network, such as a frame relay (FR) network, which includes network resources made up of networked elements and customer premises equipment interconnected by one or more physical paths, a Virtual Private Network (VPN) is built above the underlying packet-based network and includes selected portions of the packet-based network resources. The VPN is a collection of logical nodes and virtual paths (VPs) and includes one or more virtual circuits (VCs), each VC being a logical connection between VC terminators including network elements and customer premises equipment. Segments of the VCs are carried by VPs, each VP being a logical connection established between two VP terminators which are located in either network elements or customer premises equipment. One or more VPs are multiplexed on a physical path (PP). Each VP is allocated a positive guaranteed bandwidth (VP-CIR), and each VC on a VP is also allocated a bandwidth (VC-CIR) greater than or equal to zero. Packets of information to be transmitted over a VC are provided with a unique address field to thereby identify the VCs and VPs associated with the VPN over which the packet of information will travel. Congestion control of the network is provided such that congestion control and management are carried out on a per VPN basis, and congestion outside of a VPN's logical domain does not affect the performance of the VPN.

27 Claims, 8 Drawing Sheets



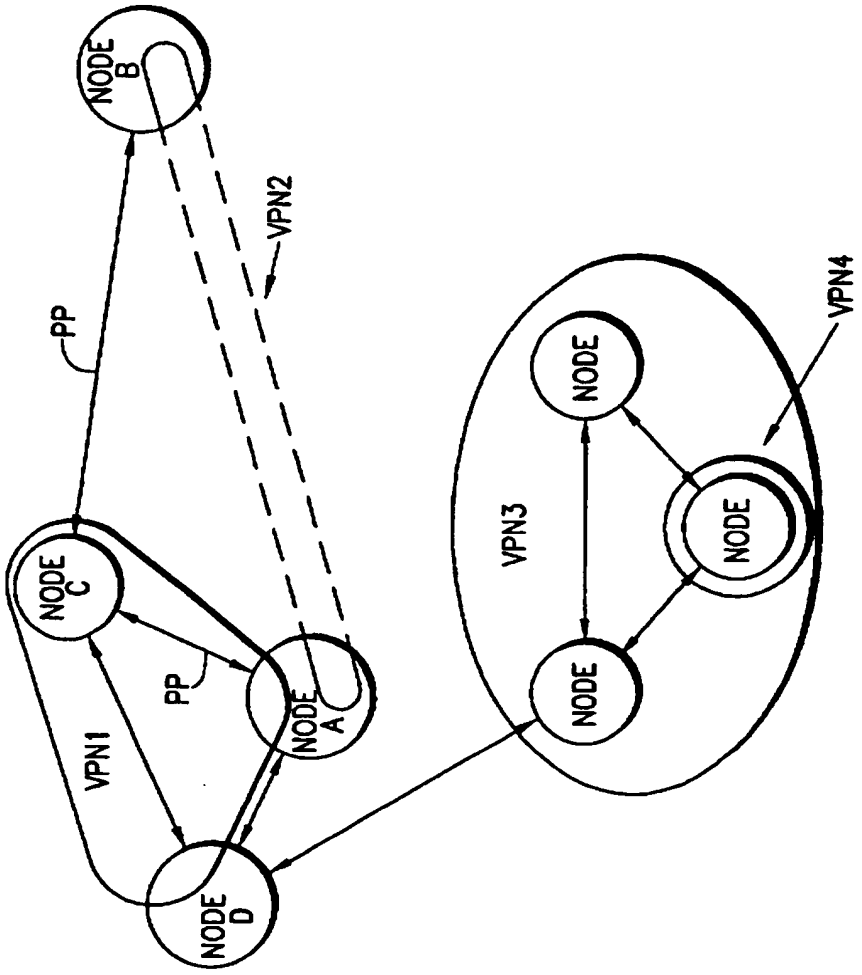


FIG. 1
(prior art)

FIG. 2

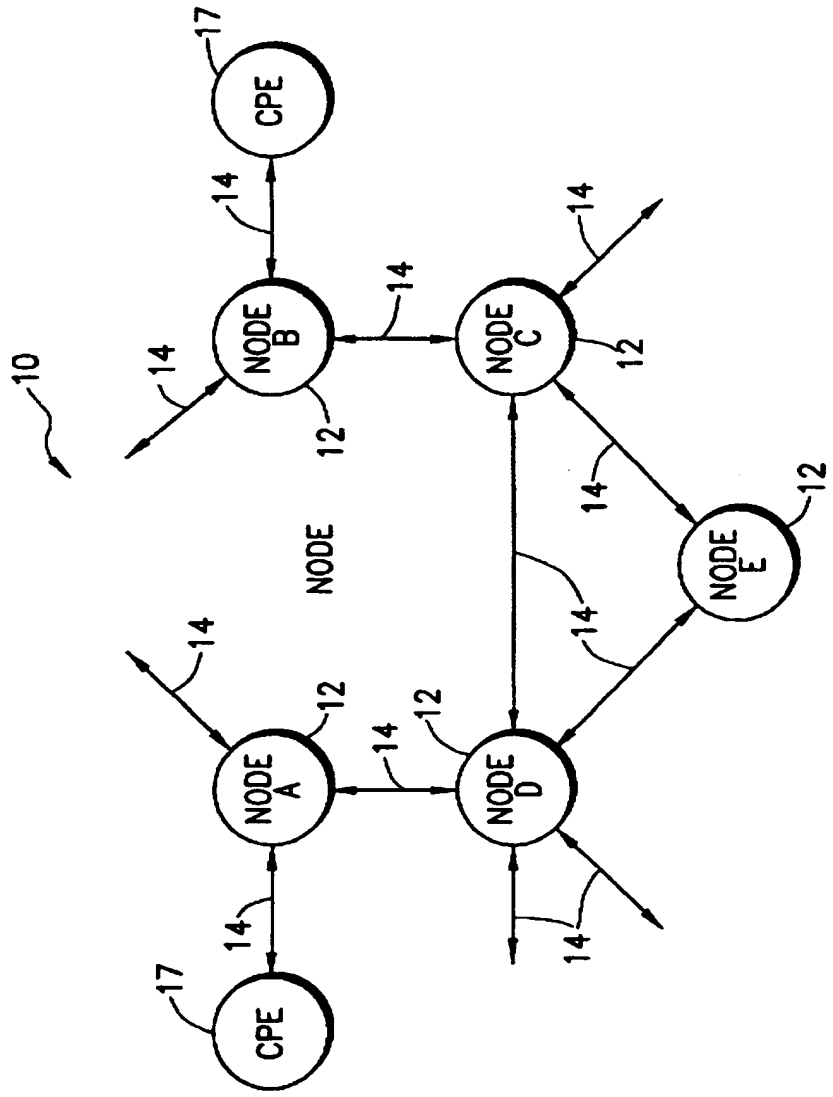


FIG. 3

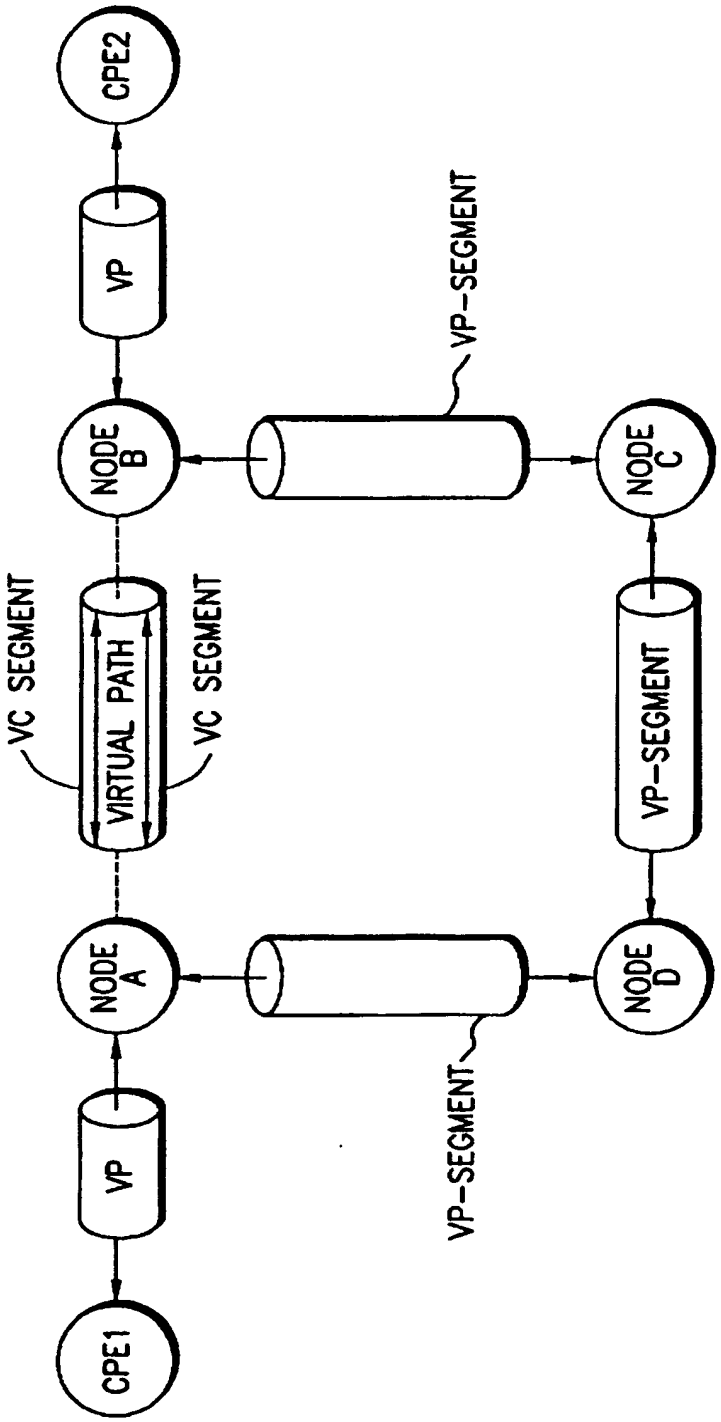

CPE2
VP
NODE B
VP-SEGMENT
NODE C
VC SEGMENT
VIRTUAL PATH
VC SEGMENT
VP-SEGMENT
NODE A
NODE D
VP
VP-SEGMENT
CPE1

FIG. 4

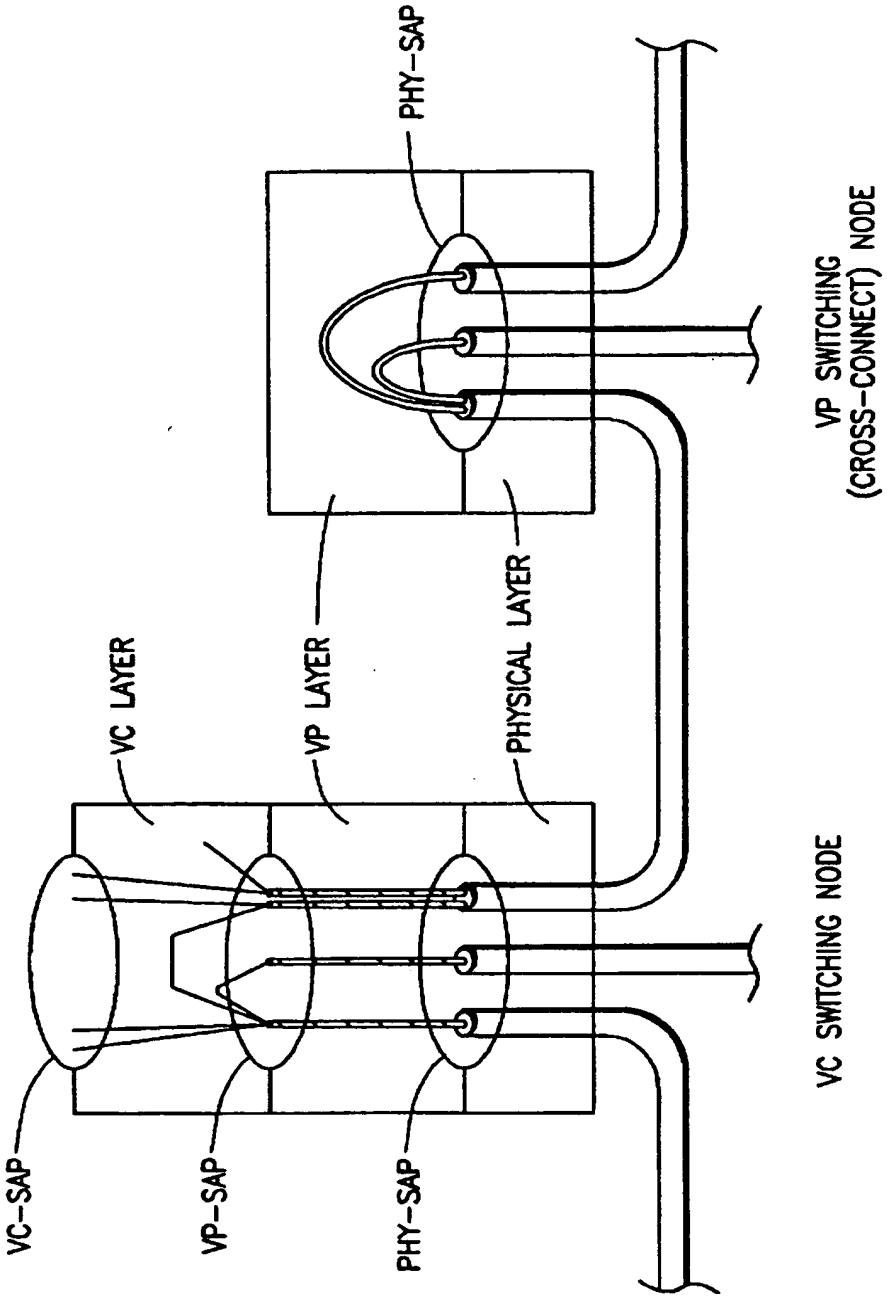

PHY-SAP
VP SWITCHING (CROSS-CONNECT) NODE
VC LAYER
VP LAYER
PHYSICAL LAYER
VC SWITCHING NODE
VC-SAP
VP-SAP
PHY-SAP

FIG. 5

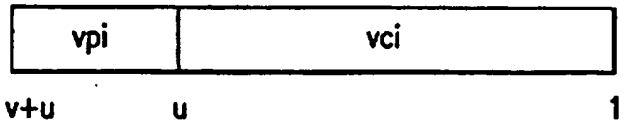


FIG. 6

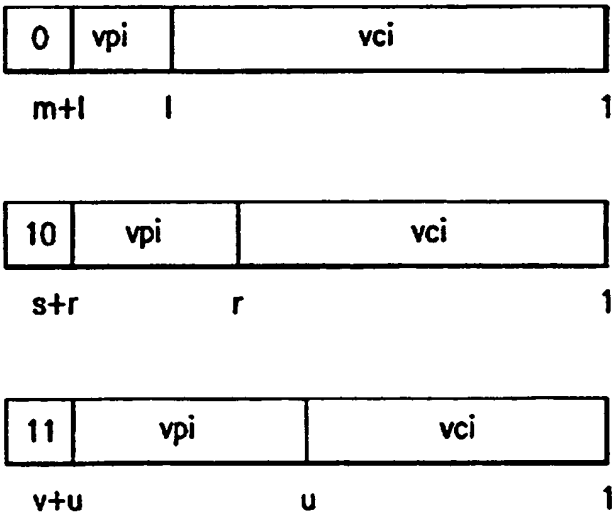


FIG. 7

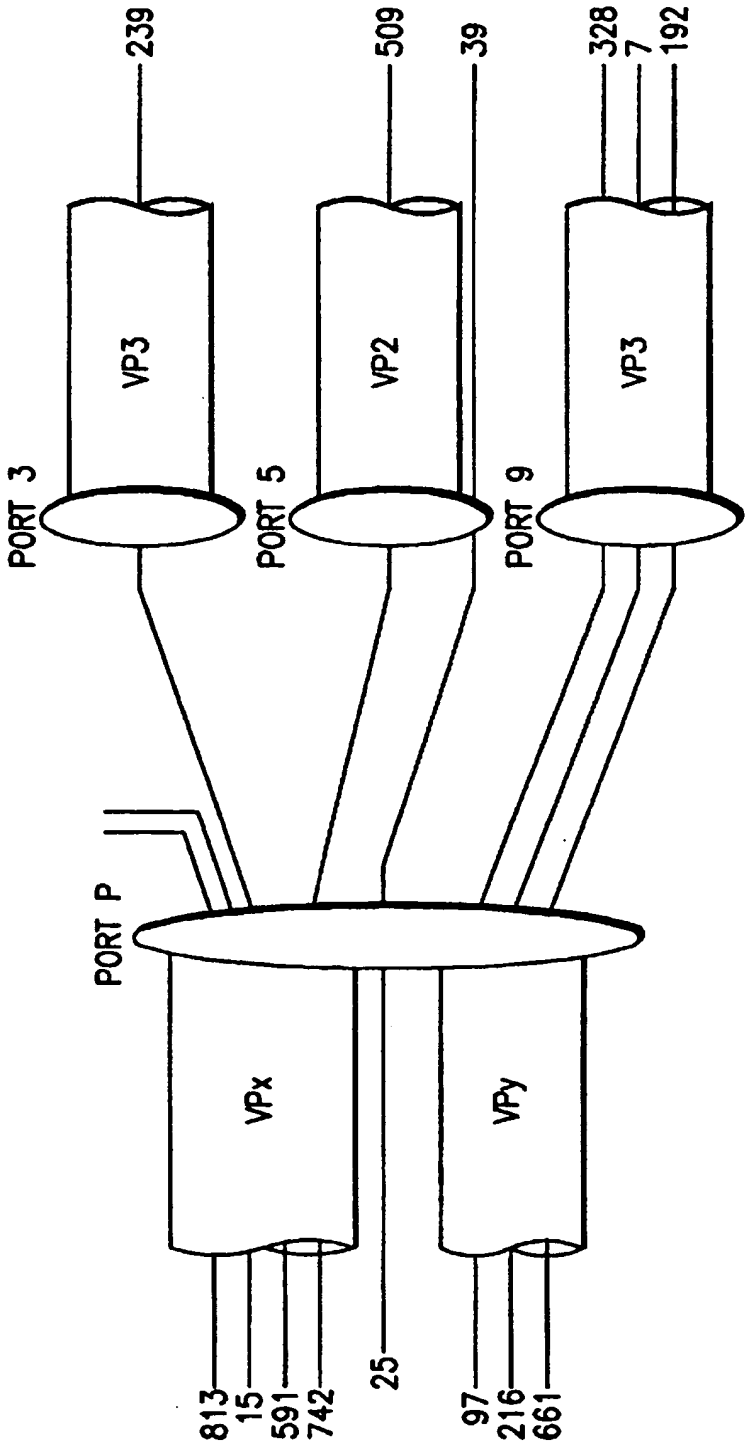

239
509
39
328
7
192
VP3
VP2
VP3
PORT 3
PORT 5
PORT 9
PORT P
VPx
VPy
813
15
591
742
25
97
216
661

FIG. 8

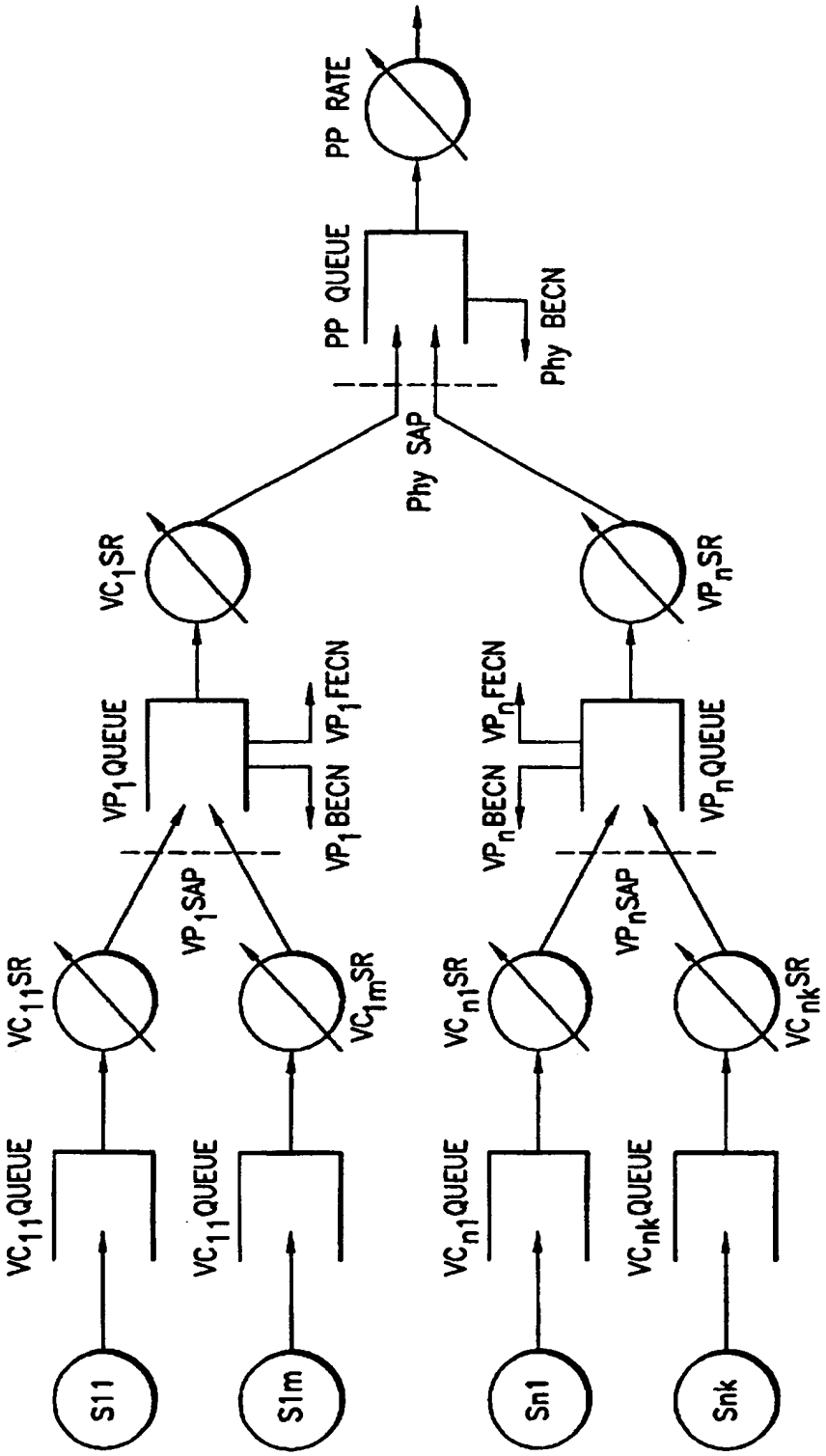

PP RATE
PP QUEUE
Phy BECN
Phy SAP
VC1SR
VPnSR
VP1QUEUE
VP1FECN
VP1BECN
VPnFECN
VPnBECN
VPnQUEUE
VP1SAP
VPnSAP
VC11SR
VC1mSR
VCn1SR
VCnkSR
VC11QUEUE
VC1mQUEUE
VCn1QUEUE
VCnkQUEUE
S11
S1m
Sn1
Snk

FIG. 9

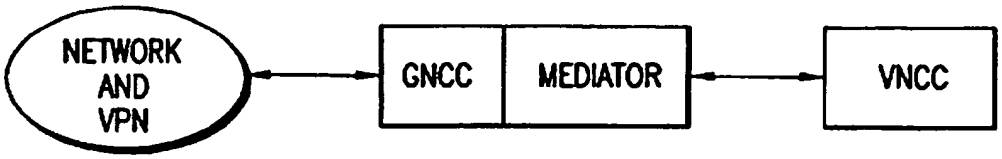
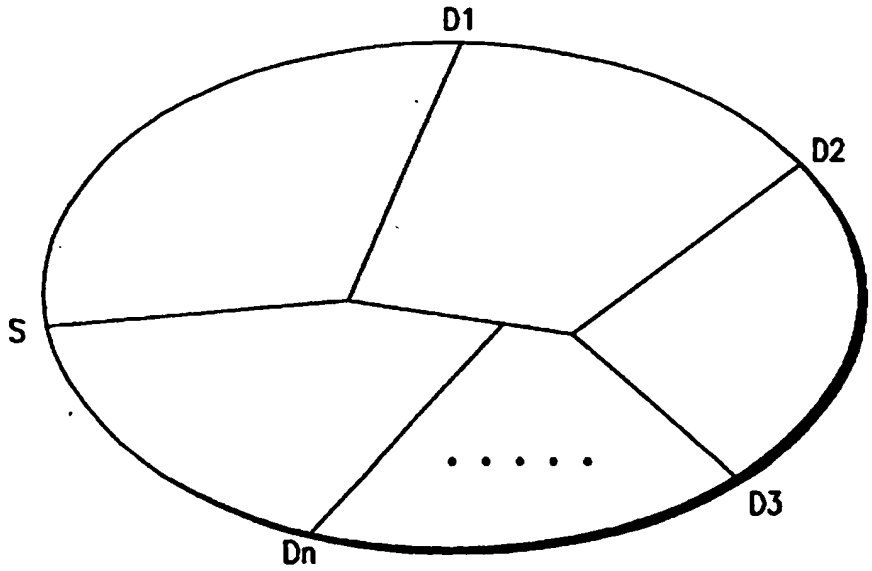


FIG. 10



VIRTUAL PRIVATE NETWORK

TECHNICAL FIELD

The present invention generally relates to packet switching (packet-based) networks, and more particularly, to logical sub-networks of a packet switching network called virtual private networks (VPN).

BACKGROUND OF THE INVENTION

Until recently, the networking choices available to a packet switching (packet-based) network customer were limited to either subscribing to some network (public or private) or becoming a private network owner. Examples of packet-based networks include: frame relay (FR) networks wherein a packet corresponds to a FR frame; a cell-switching network, e.g., an asynchronous transfer mode (ATM) network, wherein a packet corresponds to an ATM cell; etc. For small networking needs, subscription was the usual choice. Its main advantage is that it frees the customer of having to deal with engineering, operating and managing the network. In addition, since the network provider might be able to provide the service at very competitive rates compared to private purchase of telecommunication equipments, there is a potential economic saving.

How advantageous the subscription to a network might be, there are circumstances when it may be preferable to turn to private network ownership. Firstly, a customer is at the mercy of the responsiveness of the network in supporting specialized equipment, feature or function. An owner, on the contrary, has complete freedom in implementing the service and features it requires. Secondly, a customer may need specific network capabilities (e.g., in the areas of accounting and security) which are not satisfactorily available. An owner can control and enhance the capabilities for which there is desired customer support. Finally, when a customer has a large networking requirement, it may achieve better economics of scale by buying its own communication equipments.

In order to overcome the disadvantages associated with network subscription and network ownership, there is an emerging trend among network operators to sell connectivity and bandwidth in the form of Virtual Private Networks (VPN). The VPN offers a middle ground between network subscription and network ownership. Today, most often, a VPN is simply a collection of network resources taken from an underlying network. This collection can range anywhere from a set of isolated subscriber ports to a set of connected network equipment (ports, trunks, nodes) constituting a sub-network in itself.

An underlying FR network may support many VPNs, which may or may not share common equipment. Typically, the traffic generated by a VPN user is handled just as the traffic generated by any user of the underlying FR network. No network distinction is provided to the logical VPN entity. Hence a VPN will is provide the same quality of service as the underlying network. For example, if a trunk is congested because a particular connection generates too much traffic, all the connections sharing this trunk will be impacted (e.g., increase of the queuing delay and of the loss rate). There is no isolation among the traffic pertaining to a VPN, another VPN, or unrelated underlying network traffic within the FR network.

The typical VPN configurations, currently offered, are illustrated in FIG. 1.

Here, VPN1, is a collection of subscriber ports, trunks, a complete network element, and partial resources of two

other network elements. VPN1 can be viewed as a sub-network of the underlying FR network since there is connectivity within the boundary of the VPN. The situation depicted by VPN2 is that of a collection of subscriber ports and partial resources of two network elements. The VPN2 itself is not a network in the usual sense of the word. There is no connectivity within the boundary of the VPN2 between subscribers on one of the network elements and those which are connected to the other network element. Thus, VPN2 is merely a management domain of the FR underlying network. There is little or no assurance that there will be the proper amount of network resources to support the traffic or connectivity needs of VPN2. Of course, the underlying physical FR network provides the required connectivity; however, the VPN2 network manager is not permitted a clear view of the actual "network".

VPN3 illustrates a classic "private network" carved from the resources of the underlying FR network. Here, VPN3 is really its own network with the potential of semi-autonomous network management. It is possible to reserve the exclusivity of the subnetwork resources to the VPN subscribers. Note that the granularity of the reserved resources is always the entire physical resource (trunk, port). The underlying FR network provides the equipment and transmission facilities and is ultimately responsible for the overall health of the VPN. The underlying FR network assumes the burden of these tasks so that the VPN 3 manager only participates to the level to which it desires.

VPN4 is a sub-VPN of VPN3. It is included to show that VPN offerings parallel private network offerings. A sub-VPN can manage some portion of a VPN and even provide specialized services not required or offered by the remainder of the underlying VPN to which it is associated.

While a VPN provides significant advantages as described above, a drawback associated with VPNs is that most of the time a VPN guarantees only access not performance. The VPN traffic must share resources in an unpredictable way with other VPNs or non-VPN subscriber traffic. The exception is when trunking and switching capacities are reserved for the VPN and when the VPN traffic is constrained to use these capacities, e.g. VPN3.

There therefore exists a need for a virtual private network which permits VPN users to obtain a level of service generally unperturbed by the traffic generated by users outside the VPN's logical domain.

SUMMARY OF THE INVENTION

Objects of the present invention include providing an improved virtual private network (VPN) for a packet switching (packet-based) network, the VPN providing an enhanced level of management control and function to a manager of the VPN and the VPN providing a level of service which is generally independent of other traffic on the network outside of the VPN's logical domain.

According to the present invention, in a packet switching (packet-based) network, such as a frame relay (FR) network, which includes network resources made up of networked elements and customer premises equipment interconnected by one or more physical paths, a VPN is built above the underlying network and includes selected portions of the network resources. The VPN is a collection of logical nodes and virtual paths (VPs) and includes one or more virtual circuits (VCs), each VC being a logical connection between VC terminators including network elements and customer premises equipment. Segments of the VCs are carried by VPs, each VP being a logical connection established

between two VP terminators which are located in either network elements or customer premises equipment. One or more VPs are multiplexed on a physical path (PP). Each VP is allocated a positive guaranteed bandwidth (VP-CIR), and each VC on a VP is also allocated a bandwidth (VC-CIR) greater than or equal to zero. Packets of information to be transmitted over a VC are provided with an address field having local significance for identifying the respective VCs and VPs used by the VPN to which the packets of information are associated. Congestion control of the network is provided such that congestion control and management are carried out on a per VPN basis, and congestion outside of a VPN's logical domain does not affect the performance of the VPN.

In accordance with a first embodiment of the present invention, the address field includes a fixed length VC identifier field (vci) and a fixed length VP identifier field (vpi) to uniquely identify the VC and VP over which the packet of information will travel.

In accordance with a second embodiment of the present invention, the address field is made up of variable length subfields including a class-type field, a vpi field and a vci field. The class-type field identifies the length of the vpi and vci fields.

In accordance with a third embodiment of the invention, the address field is an integrated field which identifies both VPs and VCs, the integrated field being cacoded to uniquely identifying how a packet of information is switched within a node of the network. In particular, each node is provided with a connection table which identifies, for each input VC of each input VP, a corresponding output VC, output VP and output port of the node. Alternatively, the connection table will indicate if the VC is terminated within the node.

In further accord with the present invention, each VP on a PP of the network is allocated a positive guaranteed bandwidth (VP-CIR), and when congestion occurs on the PP, only those VPs utilizing bandwidth greater than the guaranteed bandwidth are required to reduce submission rate of packets onto the network. Therefore, even if the PPs utilized by a VC are congested, if the VP used by the VC is lightly loaded, the VC can utilize bandwidth at least equal to, and possibly greater than, its allocated bandwidth (VC-CIR).

According further to the present invention, the bandwidth utilization of each VP within a VPN is monitored, and when one VP is utilizing less than its guaranteed bandwidth, any excess bandwidth is equally shared among the remaining VPs in proportion to their guaranteed bandwidth with respect to the total bandwidth on the PP carrying the VP.

According still further to the present invention, a VP is established within the network locally at each node traversed by the VP by first finding an outgoing trunk from the node with available bandwidth to support the guaranteed bandwidth of the VP and able to support the number of VCs carried by the VP; reserving these resources on the PP; and updating the connection table in the node by mapping the incoming VCs and VPs to the outgoing VCs and VPs of the node.

According still further to the present invention, a VC is established within a VPN by first identifying a VP towards the destination having at least the available bandwidth required by the VC and an unused VC segment, and then reserving these resources for the VC and updating the connection table within the nodes. At the VP termination either the destination is reached or the VC is switched as described above onto a new VP toward the destination until the ultimate destination is reached

According still further to the present invention, a signaling VC is reserved on each VP for management functions.

The VPN of the present invention provides a significant improvement over the prior art. The present invention provides for the identification of packets on the network to specific VPNs. Therefore, a VPN in accordance with the invention provides a level of service generally unperturbed by traffic generated by users outside of the VPN's logical domain. The VPN concept, of the present invention, provides a natural way to offer features and functionality, normally attained only through some manner of total network ownership. Although the provision of the physical network, supporting the VPN, takes on a layer of additional complexity with the definition of VPs, the rewards gained in the specification and management of a VPN, defined in this manner, show the power of this approach. By use of the VPN concept, VPN network management becomes more than the display of random disjoint information from the underlying network. It offers the capability of providing the VPN manager with a view of the logical network to which it has subscribed, thereby permitting it to take coherent action to provide accurate and adequate support to its VPN user community.

The foregoing and other objects features and advantages the present invention will become more apparent in light of the following detailed description of exemplary embodiments thereof, as illustrated in the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic block diagram of a frame relay network having a plurality of prior art virtual private networks;

FIG. 2 is a schematic block diagram of the physical network topology of a portion of a frame relay network;

FIG. 3 is a schematic block diagram of a virtual path containing virtual circuits of the frame relay network of FIG. 2;

FIG. 4 is a schematic block diagram of a frame relay network protocol layer model;

FIG. 5 is a diagram illustrating an address field having fixed length fields for identifying virtual circuits and virtual paths;

FIG. 6 are schematic block diagrams of address fields having variable lengths fields for identifying virtual paths and virtual circuits;

FIG. 7 is a schematic block diagram showing the switching of virtual circuits within a node of the frame relay network;

FIG. 8 is a schematic block diagram illustrating the traffic policing and congestion control within the virtual private network of the invention;

FIG. 9 is a schematic block diagram showing the relationship between a general network control center (GNCC) and a virtual private network control center (VNCC);

FIG. 10 is a schematic block diagram of a virtual private network configured to support group committed information rate (CIR).

DETAILED DESCRIPTION OF THE INVENTION

For purposes of simplifying the description of the present invention, a number of abbreviations are used in the following description. The following table of abbreviations is provided as a reference for the reader:

ABBREVIATION	MEANING
Bc	Committed Burst Size
Be	Excess Burst Size
becn	Backward Explicit Congestion Notification
BVP_i	Bandwidth (VP-CIR) of the i-th VP
CIR	Committed Information Rate
CPE	Customer Premises Equipment
CPU	Central Processing Unit
EBW	Excess Bandwidth
EIR	Excess Information Rate equal to ((Bc + Be)/T) where T is Bc/CIR
dlci	Data Link Connection Identifier
fecn	Forward Explicit Congestion Notification
FR	Frame Relay
FRC	Frame Relay Connection
GNCC	General Network Control Center
neq_{vp}	Index Set of Non-Empty VP Queues
PP	Physical Path
sap	Service Access Point
SR	Service Rate
TR	Bit Rate of the Trunk
VC	Virtual Circuit
vci	VC Identifier
VNCC	VPN Network Control Center
VP	Virtual Path
vpi	VP Identifier
VPN	Virtual Private Network

The present invention provides a VPN for a FR network. The VPN is built above the underlying FR network and permits the VPN user to obtain a level of service generally unperturbed by the traffic generated by users outside the VPN's logical domain. As will become apparent to those skilled in the art in the following description, a VPN in accordance with the invention is a collection of logical nodes and virtual paths. Within the nodes of the FR network, identification information is used to uniquely identify specific traffic with a VPN. Therefore, congestion control and management can be carried out on a per VPN basis and congestion outside of a VPN's logical domain will not affect the performance of the VPN.

Referring to FIGS. 2 and 3, a portion of a typical FR network 10 is shown. The FR network 10 includes network elements (nodes) 12 interconnected by one or more physical paths (PP) 14. A PP 14 is any communications link or channel capable of supporting a virtual circuit (VC) segment between Customer Premises Equipment (CPE) 17 and a network element 12 or between two adjacent network elements 12. A VC is a logical connection established between two VC-terminators. A VC-terminator is usually located in a CPE 17, in which case the VC-terminator may be a source or destination of network traffic (data). Alternatively, a VC-terminator may be located in a network element 12, as is the case when the VC is used to transfer management data between a network element 12 and a network management center (not shown). A VC-segment is the portion of the VC carried by a virtual path (VP) between two adjacent VP-terminators. A VP is a logical connection established between two VP-terminators. A VP-terminator is either located in a network element 12 or CPE 17. A VP-segment is the portion of a VP using a particular PP between two adjacent CPEs; between a CPE 17 and a network element; or between two adjacent network elements 12.

The Committed Information Rate (CIR) is the guaranteed bandwidth available for data transfer between two endpoints of a FR network. A CIR value of zero implies that there is no guaranteed bandwidth. A bandwidth (VC-CIR) is allocated to each VC. A non-zero VC-CIR is allocated to a VC if at least a portion of data transfer is to be guaranteed. As will be understood by those skilled in the art, the minimum VC-CIR is zero, in which case there is no guarantee of data delivery. A guaranteed (positive) bandwidth (VP-CIR) is allocated to each VP.

Several VPs can be multiplexed on a PP (i.e., trunk) provided that the sum of all the VP-CIRs does not exceed the bandwidth of the PP. Usually a VP will span multiple successive PPs. Similarly several VCs can be multiplexed on a VP and, usually, a VC will span multiple successive VPs. A VP multiplexes segments of VCs under the condition that the sum of all the VC-CIRs of the multiplexed VCs does not exceed the VP-CIR. The actual paths of the VC-segments follow the PPs making up the VP.

Referring still to FIGS. 2 and 3, although there is no direct physical connectivity between nodes A and B, it is possible to create virtual connectivity between these nodes by establishing a VP between them. The VP is made up of three VP-segments (A to D, D to C and C to B) corresponding to the three PPs it uses. A VC can be established between CPE1 and CPE2 which uses the PP CPE1 to A, the VP from A to B previously established, and the PP B to CPE2.

From a bandwidth standpoint, the VP reserves a committed bandwidth VP-CIR which must be available on the three PPs it uses. Similarly, for the VC to be set up, there must be bandwidth at least equal to VC-CIR on VP CPE1-A, VP A-B and VP B-CPE2. From the two concepts of VC and VP one can now structure the FR network using a protocol layer model.

Referring now to FIG. 4, a protocol layer model of the FR network is illustrated which includes two nodes of the FR network. The FR function of a FR node is composed of three layers. The highest order layer is the VC layer. This layer performs a VC switching function (determination of outgoing VPs and analysis and translation of VC identifiers) or a VC terminating function. It provides end-to-end VCs between peer upper layers. The boundary between the VC layer and the upper layer is called VC-sap (service access point). The next layer is the VP Layer. This layer performs the VP switching or cross-connect function (determination of outgoing PPs and analysis and translation of VP identifiers) or a VP terminating function. The boundary between the VP layer and the VC layer is called VP-sap. Note that the VCs are invisible to the VP layer. The final layer is the Physical Layer. The Physical Layer provides a transmission path between adjacent VP layers. The boundary between the physical layer and the VP layer is called Phy-sap.

A node can implement the physical and VP layers only: it acts then as a VP switching (cross-connect) node. In a different configuration, a node can implement the physical layer, the VP-termination part of the VP layer and the VC layer: it acts, in this case, as a VC switching node. Finally, a node can implement the three complete layers: it acts, in this case, as a hybrid node, switching VCs and cross-connecting VPs.

A. Implementation of the VPN In a Frame Relay Network

The introduction of the VPN concept discussed above with respect to FIGS. 2, 3 and 4 impacts directly the implementation of the three planes of the FR network: transfer, control and management. The extent of the impact depends largely on the sophistication of the service provided. Following is a discussion of the three FR network planes and the implementation of a VPN in accordance with the invention with respect to the three FR network planes.

1. Transfer Plane

a. Identification of Virtual Paths and of Virtual Circuits

As described above, several VPs can be multiplexed on a PP and several VCs can be multiplexed on a VP. In order to implement a VPN in accordance with the invention, each VC within a VP must be uniquely identified at the VP-sap and, similarly, each VP within a transmission path must be uniquely identified. As described hereinafter, each node within the FR network uses the VC and VP identification information for properly switching and routing VPs and VCs. Additionally, by using such an identification scheme, the VPN can be implemented within the FR network in a manner that actions such as congestion control and management can be carried out on a per VPN basis because traffic associated with a VPN is uniquely identified. Therefore, congestion outside of a VPN's logical domain will not affect the performance of the VPN.

The Q.922 frame structure defined in *ISDN Link Layer Specification for Frame Mode Bearer Service*, ITU-T-Q.922 (formerly CCITT Q.922), 1992, the disclosure of which is incorporated herein by reference, used in Frame Relay data transfer, has an address field of 10, 16 or 23 bits, the value of which is called the data link connection identifier (dlci). In the standard Frame Relay service, this field is used as the local identifier of a virtual connection on a physical path. However, in accordance with the invention, the dlci may be used to identify VPs and VCs. In accordance with the invention, there are three alternatives for structuring and interpreting the dlci, each one achieving a particular trade-off between the utilization efficiency of the bits of the address field and the complexity of interpretation of this field. These three alternatives assume that the FR network is assembled with FR products implemented with a 2-byte control field, i.e., a dlci of 10 bits.

(1) Fixed Length Fields Identify VPs and VCs

Referring to FIG. 5, the fixed length dlci may be divided into a VC identifier (vci) of u bits and a VP identifier (vpi) of v bits. The two sub-fields have a fixed length and are always at the same place in the address field, which makes the interpretation of the dlci simple. The shortcoming of this option is that u bits are systematically reserved per VP allowing up to 2^u VCs to be multiplexed on every VP even if a much smaller number of VCs is actually multiplexed per VP. Thus the bit utilization efficiency is poor.

(2) Variable Length Fields used to Identify VPs and VCs

Referring now to FIG. 6, the fixed length dlci may include a variable length vci field and vpi field. This option overcomes the limitations of the fixed length fields. The address field is structured in 3 subfields: a class type subfield, a vpi subfield and a vci subfield. The class type (the first 1 or 2 bits of the address field) indicates the size of the two remaining fields.

FIG. 6 illustrates the application of this scheme to identify three classes. In this example, the three class type fields, with binary values 0, 10 and 11, indicate that on a single trunk (physical path) one can multiplex 2^m VPs bearing 2^1 VCs; 2^8 VPs bearing 2^r VCs; and 2 v VPs bearing 2^u VCs, respectively. This scheme allows a more efficient usage of the bits of the address field by adapting the vpi field size to the real user needs, while keeping the interpretation function quite simple.

(3) A Single Integrated Field Identifies VPs and VCs

The two preceding options for identifying VPs and VCs have two possible drawbacks. First, both the fixed length and variable length options assume that the VPN concept is generalized throughout the underlying network and that each node can correctly interpret the address field. It is more likely that only a fraction of the resources of the network will be dedicated to VPNs, the other fraction being used by non-VPN subscribers. Secondly, most FR switches process address fields of 10 bits. Thus it is hard to simultaneously satisfy the need for a large number of VPs each carrying a large number of VC segments. Therefore, another identification scheme is provided in accordance with the present invention which enables the coexistence of VPNs and the original underlying network and provides the flexibility to handle the needs of them both, whereby there is no specific sub-field identifying a VP within the address field. On the contrary VP and VC identifiers are merged into a unique field which is correctly interpreted in the network elements by way of a proper encoding of connection tables.

A FR node can play the three roles of: (1) FR connection switch; (2) VP cross-connect whereby a VP is switched as a global entity (i.e., the VCs bundled in the VP are not visible); and (3) VC-switch whereby an ingress VP is terminated with its multiplexed VCs unbundled. These VCs are then either terminated or switched to egress VPs.

FIG. 7 illustrates a situation encompassing the three roles of the node. As a VP cross-connect node, it switches a VP identified as an ordered pair, e.g., ordered pair (ingress VP y, port p) is switched to (egress VP 3;, port 9). The three VCs multiplexed on this VP are identified by the dlci values of 97, 216 and 661 on the ingress VP-segment and by dlci values of 328, 7 and 192 on the egress VP-segment. In the following connection table, these three VCs are bound together by a triplet (ivpi, evpi, eport) which has the value (y, 3, 9) in this case.

INGRESS PORT CONNECTION TABLE

idlci	ivpi	edlci	evpi	eport
15	x	—	—	—
25	—	39	dvpi	5
97	y	328	3	9
216	y	7	3	9
591	x	239	3	3
661	y	192	3	9
742	x	509	2	5
813	x	—	—	—

As a VC-switch node, it terminates ingress VP x and considers, one by one, the four VCs multiplexed on this VP. Two VCs (with idlci values of 813 and 15) are terminated in the node, identified by the fact that the triplet (edlci, evpi, eport) is Nil for each. The two others (with idlci values of 591 and 742) are switched and multiplexed with new dlci values on different egress VPs (239, 3, 3) and (509, 2, 5) respectively.

Finally, as a standard FR connection switch, the node switches a connection identified by ingress dlci 25 on ingress port p to egress dlci 39 on egress port 5. In this case, the evpi value is denoted by the special value dvpi, associated with all standard FR connections. The purpose of this dvpi designation will be explained in greater detail hereinafter.

Each connection, whatever its type (VP, VC or standard FR connection), is identified on the PPs by the dlci. It is the connection table, present only at each VP-terminator port, which maps the dlci to its specific role. In transit nodes, the normal routing processes for FR frames are used. All the bits in the address field of the frame are used efficiently without a noticeable increase of the complexity of interpretation of this field during the actual data transfer. Once the connection has been configured properly and a connection table is established (as described hereinafter), the switching

function can take place using each dlci as described in the examples of FIG. 7 and with respect to the connection table above.

A frame with the dlci 813 is received on the ingress port (ivpi) p. Since the fields edlci, evpi and eport, corresponding to the entry 813 in the connection table, are set to Nil, this connection (and the VP it is multiplexed on) is terminated in the node. Therefore the frame is delivered to the upper layer.

A frame with the dlci 591 is received on ivpi p. The fields edlci, evpi and eport, corresponding to the entry 591 in the connection table, indicate that the frame must be forwarded on the egress VP (evpi) 3 of egress port (eport) 3 with an egress address field (edlci) set to 239.

A frame with the dlci 97 is received on ivpi p. The fields edlci, evpi and eport, corresponding to the entry 97 in the connection table, indicate that the frame must be forwarded on evpi 3 of eport 9 with edlci 328.

A frame with the dlci 25 is received on ivpi p. The fields edlci, evpi and eport, corresponding to the entry 25 in the connection table, indicate that the frame must be forwarded on evpi dvpi of eport 5 with edlci 39.

It will be noted that, in the above cases, the processing of a frame is unique, irrespective of whether the frame belongs to a VC, a VP or a standard FR connection. In this respect the switching function is integrated.

(4) Increased Length Address Field

As discuss above, with a 10 bit address field, it may be preferable to implement a single integrated (encoded) address field for identifying VPs and VCs because of the drawback associated with both fixed length and variable length address fields. However, this solution could be reconsidered if the address field becomes 16 or 23 bits long. In this case, the size of the connection table in each port (2^1 where 1 is the length, in bits, of the address field) becomes unacceptably large. At the same time, the need for efficiency of bit utilization of the address field associated with this embodiment disappears.

With a longer address field, the variable length field approach described above may be preferable to an integrated address field. For example, the above described variable length address field may be provided with a fixed length class type field. For example, with a 2-bit class type, one category (e.g., class type having binary value 00) could be used to identify those connections which are unaffiliated with a VPN. The other three class types, i.e., binary values 01, 10, 11, would then be associated with three different sizes of vpi as described in the variable length discussion.

An immediate benefit of the size of the connection tables using this modified variable length approach is that a pure VP cross-connect node needs to deal only with the vpi portion of the address field, enabling drastic reduction of the size of the connection table. Another benefit is that a hybrid node (VP cross-connect and VC-switch) can process the address field in two stages, an evaluation of the pi followed, only when the VP is terminated, by an evaluation of the vci. The size of the connection table will be significantly reduced since at any port only a small number of VPs are actually terminated. Finally, for a node dealing with standard FR connections, the size of the connection table is determined by the number of significant bits in the address field for class type 00.

(5) Summary of the VP and VC Identifiers

Three different schemes for identifying VPs and VCs in accordance with the present invention are described above. For a short address field, i.e., 10 bits, it may be preferable to use a single integrated (encoded) address field for identifying VPs and VCs. However, for longer address fields, e.g., 16 or 23 bits, it may be preferable to use a variable address field with a fixed length class type field. As will be understood by those skilled in the art, all that is required in order to implement the VPN of the present invention is a method to properly identify VPs and VCs within nodes so that traffic may be properly routed and associated with appropriate VPs and VCs for purposes of traffic management and congestion control.

b. Traffic Management and Congestion Control

Traffic management and congestion control are two tightly related functions of the FR transfer plane. With the introduction of the VPN concept, the traffic management and congestion control functions must be implemented at several levels in the network as illustrated in FIG. 8. The following discussion relates to backward congestion notification processing, the notification to a source of a data stream, e.g., a VC-terminator, that there is congestion along the VP within the VPN. The forward congestion notification processing, e.g., the notification of congestion to a destination of a data stream, is handled analogously. The VPN of the present invention provides improved traffic management and congestion control because traffic associated with a specific VPN is uniquely identified within the FR network. Therefore, the traffic management and congestion control in accordance with the invention is implemented such that the traffic within a given VPN is unperturbed by traffic generated outside of the VPN's logical domain.

(1) Traffic Management at the Phy-sap

All the frames to be transmitted on a transmission trunk (PP) are multiplexed on a physical service access point (Phy-sap). For the sake of simplicity, channelized trunks are not considered here, although this option is not excluded. The traffic management function at the Phy-sap is illustrated with a queue representation, PP QUEUE.

The role of congestion management at the Phy-sap in accordance with the invention is to ensure that each VP is allocated at least VP-CIR for data transmission over the trunk (PP). Therefore, if congestion occurs on the PP, there will be sufficient bandwidth such that each VPN can at least transmit traffic at VP-CIR on the PP. If a PP is carrying FR traffic other than VP traffic, the total allocated bandwidth on the PP must ensure that each VP is guaranteed at least VP-CIR. Therefore the sum of each VP-CIR and CIR for other FR traffic on the trunk must not exceed the total bandwidth of the PP. If congestion occurs, then only those VPs (or other FR traffic) in excess of their corresponding CIRs must reduce submission rate onto the PP.

The unique queue (PP QUEUE) served at the physical path rate (PP RATE) is associated with the Phy-sap. The PP QUEUE is shared by all the VPs multiplexed on the egress trunk. Its maximum length, i.e, the maximum amount of data stored in the queue and waiting to be transmitted onto the PP, is determined from the maximum allowed sojourn delay and from the service rate (PP RATE) of the queue. A congestion threshold is defined which, when reached, triggers a congestion notification procedure. As long as the aggregate incoming rate is lower than the PP RATE, the queue will remain almost empty. In this case, the queue exists only to absorb the jitter due to packet clustering, a phenomenon inherent to a packet-based network.

When the aggregate incoming rate is sustainably higher than the trunk rate, congestion builds up and a physical path backward explicit congestion notification, Phy-becn, must be issued toward the VP originators. It is important to note

that, in order to provide a good isolation of traffic between VPNs, the Phy-sap congestion notification must be received by the VP originators. As a matter of fact, a few of the VPs multiplexed on the Phy-sap may be generating traffic at a rate equal or lower than their CIRs and thus the congestion should remain invisible to their VCs. Only the VPs contributing more than their VP-CIRs must reduce their traffic.

From an implementation point of view there are, potentially, several ways to notify the congestion. As described above, one way is by defining an additional bit (Phy-becn) which is set in all frames transiting in the reverse direction of a congested trunk. This bit is examined by the VP originators. Alternatively, a signaling frame (as described for example in CLLM in ITU-T-Q.922, the disclosure of which is incorporated herein by reference) may be defined which is transmitted by the physical layer toward all originators of the VPs multiplexed on the Phy-sap.

(2) Traffic Management at the VP-sap

All the frames to be transmitted on a virtual path are multiplexed on a virtual path service access point (VP-sap). FIG. 8 illustrates the traffic management function at the VP-sap with a queue representation, VP QUEUE. The traffic of a VP must be considered globally, it cannot be separated into as many traffic components as there are VCs bundled in the VP. This new characteristic entails a new mechanism of traffic management and congestion control in the nodes of the FR network.

It may happen that the trunk bandwidth is not being totally allocated or that certain virtual paths are not fully using their VP-CIRs. In this case the excess bandwidth can be shared among the non-empty VP QUEUES. Fairness is provided by sharing the excess bandwidth in proportion of the VP-CIRs. To each VP corresponds a queue (VP QUEUE) which is served at a service rate (VP SR) equal to VP-CIR at a minimum. Let neq_{VP} be the index set of non-empty VP QUEUEs, BVP_i the VP-CIR of the i-th VP, and TR the Bit Rate of the trunk. The excess bandwidth (EBW) is expressible as:

$$EBW = TR - \sum_{i \in neq_{VP}} BVP_i$$

This bandwidth is usually non-zero since VPs are not always using their full CIRs or since the trunk bandwidth is not being completely allocated. This spare capacity is shared among the non-empty queues in proportion of their VP-CIRs. For example, a non-empty queue for VP_i has a service rate SR_i given by:

$$SR_i = BVP_i + \frac{EBW \times BVP_i}{\sum_{i \in neq_{VP}} BVP_i}$$

When a Phy-sap congestion notification (Phy-becn) is received by a VP originator, it must restrict its SR to no more than VP-CIR. Subsequently it can increase the VP SR if no more Phy-sap congestion notification is received.

The VP QUEUE is shared by all the VCs multiplexed on the virtual path. Its maximum length is determined from the maximum allowed sojourn delay and from the SR of the queue (VP_i SR). A congestion threshold is defined which, when reached, triggers a congestion notification procedure. As long as the aggregate incoming rate is lower than the SR of the queue, the queue will remain almost empty. In this case, the queue is used only to absorb the jitter due to packet clustering.

A VP is congested when the aggregate arrival rate at the VP-sap (sum of the SRs of the VCs multiplexed on the VP) is higher than the current SR of this VP's queue. Congestion is detected when the VP's queue length goes beyond a congestion threshold. A strict determination of this threshold should consider the SR of the queue, the round-trip-delay user to queue, and the maximum allowed sojourn delay of a frame in the node. For simplicity this threshold may be set to a few frames (e.g. 10 frames).

When a VP is congested, the frames exiting the VP's queue towards the PP have a VP forward explicit congestion notification (VP-fecn) bit set to notify the destination of the congestion. Additionally, the frames arriving on the reverse direction on the VP (assuming bidirectional VPs) have their becn (VP-becn) bit set. Each VP is structured to guarantee bandwidth to each VC at least equal to VC-CIR. Therefore, when a VP is congested, only those VCs that are transmitting traffic onto the VP at a rate greater than VC-CIR must reduce their submission rate. In response to VP congestion, VCs will reduce their submission rate in steps until the VP congestion is cleared. However, each VC will be able to utilize bandwidth at least equal to VC-CIR.

As discussed above with respect to a single integrated address field, an ingress VP identity for the incoming frame is given by the field ivpi in the connection table. The VP concept allows the isolation of traffic of one user (or VPN) from the traffic of another user (or VPN). As will be understood by those skilled in the art, one VP, VP_i, can be congested while another VP, VP_k, sharing the same trunk is not congested. Simultaneously, the configuration of the invention allows a (non-congested) user to have a VP SR higher than the VP-bandwidth it has reserved. This situation occurs when the network is not heavily loaded.

(3) Traffic Management at the VC-sap

As in any network providing a standard FR service, the access node must implement a policing function on a virtual circuit basis, in which it monitors the incoming rate and ensures that the traffic adheres to the standard limits specified by the traffic descriptor associated to the virtual circuit (Bc, Be, VC-CIR). In addition it shapes the traffic submitted to the network as a function of the congestion notifications received from the network. Therefore, a data stream received from a source, S_{nm}, (i.e., the m^{th} VC of this VP_n) is initially buffered in a VC QUEUE. Thereafter, based on the condition of the network as described above, traffic is provided to the VP_n at a variable service rate, VC_{nm}SR.

Note that for a given VC, the access node S_{nm} (and the source traffic) sees only the congestion notifications (VP-becn) related to the VPs used by it. In a typical situation all the PPs along a VC are congested. But, if the VPs used by the VC are lightly loaded, this VC has a current service rate (VC SR) that can be substantially higher than its VC-CIR. This example illustrates the isolation of traffic that can be achieved by application of the VPN concept in accordance with the invention.

C. Transfer Plane Summary

There are several aspects of VPN operation that may be derived from the above-described concepts of identification of VCs and VPs, and traffic management and congestion control. Firstly, depending on its place in the network, a node can implement one or all of the three levels of traffic management described above. A pure cross-connect node (i.e., VP switch) will implement only the Phy-sap-level, a VC-switch node will implement the VP-sap and the Phy-sap levels, whereas an access node will implement all three levels. Alternatively a single node can be an access node for some VCs, a cross-connect node for some others, and a VC-switch for the remainder.

A network can dedicate part of its resources to VPNs and part to standard FR connections (for non-VPN customers).

All standard FR connections multiplexed on an egress port are associated with a pseudo VP. with the ideatifier dvpi. and to a queue. e.g., VP_{dvpi} QUEUE. This queue is served at a rate at least equal to:

$$VP_{dvpi}SR = \sum_{i \in N(dvpi)} UCIR_i$$

where N(dvpi) is the index set of all VCs belonging to the pseudo-VP and $UCIR_i$ is the VC-CIR of the i-th such VC.

The congestion control approach discussed above calls for the introduction of a Phy-becn bit and the use of the becn bit (interpreted as a VP-becn indicator). If there were a free bit in the frame header to introduce the Phy-becn notification. then implementation of the congestion notification would be straightforward. However, in standard FR frames, no such bit can be found. Therefore, in order to implement the proposed congestion notification scheme in accordance with the present invention, one could provide an additional byte to the data portion of frames at the network ingress VC-terminator. The egress VC-terminator removes the extra byte before transmitting the data to the destination device. This byte could be used to hold the Phy-becn bit which. when set, would be used by the VP originators to determine the congestion state of the VP. If it is congested, the VP originator sets the VP-becn (becn) bit on all VCs which exceed their reserved CIR. This bit, once set, remains set for the VC no matter the congestion state of other VPs which it sees. The Phy-becn bit is cleared in any event. If this implementation approach were used, then it could be possible for VP terminators to use the extra bits in the new data byte for VC identification. The header address bits could be used for the VP ideatifier. In this way, all switches in the physical path used to carry the VP could switch on the VP identifier only.

2. Control Plane

a. Routing

In a virtual private network there exists two levels of routing, one for virtual paths and one for virtual circuits. These two levels are described successively hereafter.

(1) Routing Virtual Paths (establishment of a VP)

A VP is defined by the same set of parameters as a standard FR connection (FRC), e.g., destination address, Bc, Be and VP-CIR. The endpoints of a VP may be access nodes or transit nodes. The establishment of a VP is a distributed process. Each node along the route uses routing tables describing the physical network to select the next trunk toward the destination. The node reserves on this trunk the resources required by the VP and, finally, it updates the node's connection table.

As discussed above, there is no explicit field within the frame address field to identify VPs and VCs. A VP is identified implicitly by an appropriate coding of the connection tables. As a consequence, it is necessary to know beforehand how many VCs could be multiplexed on the VP. Each VC multiplexed on the VP has an entry in the connection table. All the VCs of a VP are bound together by the common fields ivpi, evpi and eport used for traffic management purposes.

The routing of VPs can be a natural extension of normal FRC routing in a Frame Relay network. For example, suppose the FR network has an automated scheme for determining a path for a FRC. Each is configured by merely specifying the FRC endpoints (e.g., by specifying the physical network locations and the ingress dlci and egress dlci) together with the required FRC-CIR (and perhaps other performance criteria). The path selection mechanism then tries to find a path which meets the performance criteria. The chosen path is composed of FRC-segments which traverse PPs each of which has sufficient resources available to ensure that all the performance requirements are satisfied (most particularly, the FRC-CIR).

A VP is simply a special case of a FRC in the following sense. The VP is bounded by VP-terminators as endpoints (corresponding to the FRC-terminators except that, typically these VP-terminators are not subscriber ports). A VP can be specified analogous to an FRC with the addition of two parameters of operation: (1) the identity of a VPN (or reserved subscriber) to which the VP belongs; and (2) the maximum number of VCs that may be multiplexed on this VP.

When a VP setup is required, just as FRC setup reserves bandwidth on PPs with sufficient CIR, the same path selection logic can be used to select PPs which satisfy the CIR requirements of the VP. In a given cross-connect node, once an egress port with enough resources has been found, the connection table is updated. Referring again to FIG. 7, suppose, for example, three VCs can be multiplexed on the VP, the egress port selected is port 9, and the three available egress dlci values selected are 328, 7 and 192. Locally the VP which is to be set up will be identified by ivpi y and evpi 3. Three entries are reserved in the ingress port connection table and updated appropriately with the information provided above. The involvement of the node in the establishment of VCs on this VP stops here. If the VP is bidirectional, it is convenient to use the same routing information in both directions, i.e., for each entry of the connection table at the ingress port, there must be a symmetrical entry (edlci, evpi, idlci, iport) in the connection table of the egress port to describe the reverse path direction.

To summarize, the process of setting up a portion of a VP (with required CIR and bearing capability for up to n VC segments), done locally in each node traversed, consists of: (1) finding an outgoing trunk with an available bandwidth no smaller than VP-CIR and with at least n unused dlcis; (2) reserving these resources; and (3) updating the connection table by mapping an incoming dlci to an outgoing dlci and an evpi for every VC segment.

(2) Routing Virtual Circuits

The set of VPs established for a customer constitutes the customer's virtual private network. The VPN topology can be quite different from the underlying global FR network topology. The VPN nodes, which are VC switches only (cross-connect nodes are invisible to the VPN), are linked by VPs. Each VP is defined by its bandwidth (the VP-CIR) and the maximum number of VCs multiplexed on it. Moreover, each VC segment is identified by a dlci at the ingress and at the egress of the VP.

When a VC has to be established on a VPN, e.g., VPN_i, the same sub-tasks performed for establishing a VP have to be carried out in the VPN_i nodes. First, a VP belonging to VPN_i toward the destination and having at least the available bandwidth requested by the VC and an unused VC segment (i.e., an unused dlci) must be found. These resources must be reserved and the connection table updated. The connection is updated as described above with the additional requirement that the egress vpi (evpi) must be selected and identified as belonging to VPN_i.

The VC setup procedure offers varying degrees of automation. For example, if the manager of the underlying FR network selects a completely manual approach, it performs off-line the above first two sub-tasks from its knowledge of the VPN topology and state. Then it updates remotely the connection tables in each node along the VC route according to the configuration chosen.

Alternatively, the FR network manager may elect to build the routing tables corresponding to the VPN topology off-

line and download this topology into the nodes. The three routing sub-tasks are performed in a distributed way. In this case the FR network manager configures the VPs for the VPN. Once the VPs are configured, the switches (nodes) in the network automatically perform the routing sub-tasks for the VCs. This requires adjacent VP nodes to be interconnected by a signaling link on which are transmitted the messages they exchange, as described in greater detail hereinafter.

The network manager may also elect to completely automate the VC setup procedure. This encompasses, in addition to the three routing sub-tasks, a distributed function to build and maintain the routing tables specific to the VPN. This function limits itself to describing the VPN topology. In particular, the FR network manager need only specify the end points of each VP. Thereafter, the VPs and VCs are automatically routed. As described above, in specifying (defining) the end points, the FR network manager must (1) determine the specific end point locations; (2) provide the identity of a VPN to which the VP will belong; and (3) provide the maximum number of VCs that will be multiplexed on the VP. Only the nodes belonging to the VPN under consideration are active in this task. The accomplishing of the three sub-tasks is performed in a distributed way with adjacent VP nodes communicating with each other by means of a signaling link, as described below.

b. Signaling

The nodes of a VPN need to exchange messages among themselves. These messages are related to the VC-setup, supervision and tear down functions. These messages can also be related to VPN management functions (e.g., monitoring of a VP).

The most convenient way to allow this exchange of messages is to associate a signaling VC to each VP. This connection is established between the two terminators of the VP. This special VC can be multiplexed on the VP along with user VCs or it can use a physical route totally different from that of the VP. Of course, a suitable protocol must exist at the two ends of the signaling VC in order to provide a reliable exchange of information between the two VP nodes.

3. Management Plane

a. Introduction

The VPN of the present invention allows improved management functions to a VPN network manager. These management functions naturally interact with the management of the underlying FR network.

Referring to FIG. 9, and in accordance with the invention, there is a distribution of responsibilities between a General Network Control Center (GNCC) and a VPN Network Control Center (VNCC). The GNCC has complete control over the underlying FR network. This includes the control over the resources allocated to the VPN. The VNCC has a knowledge limited to its VPN. This knowledge is in terms of virtual resources (VPs, VCs, VPN topology, etc.). The operator of the VNCC is unaware of the actual resources (e.g., cards, transmission lines) used in the FR network and it has no direct access to the FR devices.

A mediation function, located between GNCC and VNCC, enables communications between the two entities. In the direction GNCC to VNCC, the mediation function filters the messages received from the network (alarms, statistics, accounting, etc.), and passes to the VNCC, in proper format, only those messages to which the VPN has involvement. In the direction VNCC to GNCC, the mediator screens VNCC messages to ensure that they are properly formatted and restricted to the VPN's virtual resources and are confined to the management level appropriate to the allowed VPN management capabilities.

The tasks of the mediator could be complex since this system must translate the physical information from the underlying FR network to the logically configured VPN with its VPs often not directly corresponding to actual equipment in the FR network. However, in order to establish VPN VPs in an automated manner, the network elements must have sufficient knowledge of the VPN virtual structure. With this information, they can determine the condition of VPN VPs, and send appropriate event information about VPN VP- and VC-related conditions with sufficient additional data to permit the mediation function to become straightforward.

b. Network Management Functional Areas

Management activities carried out by the GNCC and VNCC can be broken down in five functional areas; configuration, fault, accounting, performance and security management.

(1) Configuration Management

The configuration management functional area is composed of three main tasks. The first task involves the creation of a graphical topology of the FR network and each VPN, including a representation of the network elements, their connections and their logical position. This description may have several levels of abstraction. It allows the Fault Management to display graphically network events to the operator, e.g., FR network events to the FR network operator, and VPN events to the appropriate VPN operators.

The next task includes the specification of configuration parameters. All the elements of each VPN (including VPs, VCs and FR switching equipment) are described parametrically. The parameters drive tabular representations used by network elements to specify their environment and capabilities. The framework for the specification is a (graphical) representation of the FR network.

The third task involves the downloading of configuration parameters to the nodes (switches). This task allows each switch to initialize in its correct configuration.

The GNCC performs all these tasks for the whole network . On one hand, a VNCC may have no configuration management capabilities. On the other hand, it may provide varying configuration management functionality to its VPN (up to and including total management), but only under the ultimate control of the GNCC (through the mediator).

(2) Fault Management

This function provides for the detection and correction of abnormal network operations through the collection of information about events that affect the state of switch resources. The GNCC receives alarms and statistics from the network switches. This information is processed by fault management applications and is used to present fault indication on the graphical network topological view. Some degree of fault resolution can be initiated by GNCC-resident applications driven by operator input or by automatic invocation in response to specific alarm and statistical information.

The faults affecting the VPN are converted into VPN-level faults. For example, if a physical line in the network goes down, the fault may be converted to one or more VP failures to be sent to the VNCC as VPN faults. (It may be the case that a physical line failure does not generate any VP failure faults especially if the underlying networks has been able to reroute the VCs without disturbing the VP-terminator ports. In this case the VP appears to be functioning normally.) The VNCC fault management applications present this information as fault indications on the graphical topological view of the VPN.

The VNCC may undertake VPN fault correction actions. These actions are screened and translated by the mediator. Appropriate actions are forwarded to the GNCC which

actually initiates the fault resolution communications with network elements.

(3) Accounting Management

This function collects the data regarding the usage and accounting, so that users can be billed. The VPN is a single customer from the point of view of the billing function. However, the VPN resources are shared among several VPN users who may need to be billed individually by the VPN administration. To provide this capability, the GNCC forwards the accounting records involving VPN usage through the mediator (which converts the records to an acceptable format) to the VNCC. The VNCC takes the necessary actions to drive the billing of the VPN's individual users.

(4) Performance Management

Performance Management collects data regarding switch resource performance levels and identifies the problems useful for network configuration, analysis, trending and planning. There are two types of performance information of interest. The first type is historical information which is vital to spotting network trends with regard to traffic patterns, congestion, line quality, hardware deterioration, etc. The second type deals with almost real-time data, useful in fault diagnosis and resolution.

Typically, the network elements report historical information to the GNCC as statistical data. The GNCC/mediator scans the statistical information and assemblies the data pertinent to the VPN for formatting and shipment to the VNCC. The almost real-time data is usually resident in the network elements. This information is obtained by query from the GNCC. For VPN-related data, the VNCC must query the network elements. The underlying network administration has the responsibility of ensuring that the VNCC operations are in no way permitted to obtain unauthorized transmittal of data not directly concerning the VPN. Therefore, VNCC queries are translated and screened by the mediator and passed to the GNCC for ultimate transmittal. Alternatively, the network elements may have sufficient screening capability to permit VNCC queries to be made directly. In this case, each network element must only allow queries for information appropriate to the VPN.

(5) Security Management

Security Management controls the access, the scope and the activity of network managers invoking NMS actions on a given entity. The actions can range anywhere from passive monitoring of network activity all the way to active configuration and fault resolution actions. In this connection, it is incumbent on the underlying network to ensure that VNCC activities are restricted to the VPN. Even passive monitoring must be restricted so that the VNCC is not inadvertently given information outside of its sphere of operations. When the VNCC has the capability of altering the parameters of operation of its VPN, the security requirements are among the chief concerns since operations even to VPN-controlled resources could affect the rest of the network community outside the scope of the VPN.

To provide the necessary security, all VNCC activities are filtered by the GNCC/mediator before any direct network activity is launched. The GNCC is ultimately the source of any such VPN-related activities. In effect, the VNCC becomes a remote operator of the GNCC with restrictions applied just as if it were a user with restricted network access.

Alternatively, VNCC operation may be directed to a security server for access to a network element. Once the clearance to the network element has been established, the network element restricts any activity of the VNCC to just those resources under the scope of the VPN. This type of security partnership allows the VNCC to operate independently from the GNCC. But, at the same time, it introduces its own set of management challenges for the GNCC. In effect, the GNCC has lost control over part of its management domain while still retaining overall management responsibility. For this reason, security solutions which bypass the GNCC are difficult to implement and control.

B. Applications of the VPN Concept

The concept of VPN definition and management in accordance with the invention provides powerful solutions to practical networking problems. Several examples are presented as illustrations.

1. Rapid Restoration of Service

In case of a network failure (e.g., a cut physical cable bearing a trunk), all the connections impacted by the failure must be restored as quickly as possible. In a network not having the VPN VP switching capability, each individual connection must be reestablished independently from the other connections which were using the same disrupted network element.

The VP concept allows a quicker and simpler restoration. Only the VPs impacted by the network failure have to be reestablished. Once a VP has been restored, assuming that the physical network has enough resources available to establish a restored path, the VP-terminators at both ends of the VP must update the connection tables such that the VC-segment restored for each VC multiplexed on the VP can be concatenated anew with the upstream and downstream VC-segments still set-up.

There is additional dimension to this restoration process. When a VP is able to be restored, the VCs multiplexed on the VP remain intact. Thus there is no failure of the VP from the perspective of the VPN subscriber (although there is a failure from the perspective of the physical network). The management implication is that fault messages must be generated to the GNCC, but not a VNCC managing the VPN.

2. Isolation of Traffic Between Users

A fundamental principle of the VPN concept is that, on any VP, the bandwidth available to the VCs routed across the VP is at least equal to VP-CIR. Additionally, the VP bandwidth can increase up to the transmission link bandwidth when the physical path is lightly loaded.

The VPN manager has a certain freedom in the usage policy of the VPN resources. On the other hand the manager has a higher responsibility in controlling the inbound traffic of the VPN. This is illustrated in the two examples below:

a. Maximum Bandwidth in a Congested Network

If, on a given route in a VPN, only one connection is active, then this connection can use a bandwidth equal to the narrowest VP along this route. This is true even if one of the trunks along the route is congested.

With this feature it makes sense for a VC to subscribe to an Excess Information Rate (EIR) equal to the VP-CIR. Once the VC has reached its maximal rate EIR, it can transmit continuously at this rate even on a highly loaded network as long as none of the VPs transited require a decrease due to congestion. Even when such a decrease is necessary, the VC is still guaranteed a transmission rate of VC-CIR.

It is the responsibility of the VPN manager to specify the maximum allowed usable CIR on a VP, a percentage of the VP-CIR. Multiple VCs can be carried on a VP so long as the sum of their VC-CIRs do not exceed the usable VP-CIR. In this manner individual VCs carried by the VP may exceed their individual VC-CIRs for bursts without causing VP congestion.

b. Grouped CIR

The concept of the Grouped CIR (statistical CIR) feature relates to the CIR's of a group of connections at a single access point. Several connections are established from the single access to several destinations, the sum of their CIRs is higher than the access rate. Thus the VCs emanating from this access at any point in time have an aggregate (or 'Grouped') CIR bounded by the access rate. By considering all of these VCs as a group, the transit network needs to allocate no more than the access rate for CIR even if the sum of the individual CIRs of the VCs in the group exceed the access rate. The VP carrying such a VC group has less CIR requirement than would be necessary if it treated the VCs of the group individually.

Referring to FIG. **10**, the VPN concept of the present invention provides a graceful way to support this Grouped CIR feature and to extend it. For example, a client has n connections to establish between a single access and n distinct destination. At any given time the source does not generate a rate higher than X kbps (X kbps being equal to the access rate or to a lower value). To satisfy this requirement one creates a VPN as illustrated in FIG. **10** where, for each VP, a bandwidth equal to X kbps is reserved. Then n zero-CIR connections are established, one from the source (S) to each of the destinations (D1, D2, . . . , Dn) on this VPN. As long as the aggregate rate at S is not higher than X kbps, the traffic submitted to the VPN will be transmitted without discard.

Several variants to this basic scheme are possible. For example each VC, with source at S, has its own CIR. In this case the VP-CIR reserved for a given VP should be equal to: min [X kbps, ΣCIR of VCs multiplexed on the VP].

The grouped CIR feature can be extended to the case of multiple sources. The requirement is that the aggregate bandwidth reserved on any trunk for the n connections originating from multiple sources cannot exceed X kbps.

The grouped CIR feature can be extended to the case of multiple sources each converging on a single egress access line of bandwidth Y kbps. In this case, a VPN can be established in a manner similar to FIG. **10** (treating S as the egress access and D_1, D_2, . . . Dn as the sources). The VP-CIR reserved for each of the VPs in the VPN is set equal to: min [Y kbps, ΣCIR of the VCs multiplexed on the VP]. By so limiting the VP-CIRs, no more than Y kbps of traffic will ever be transmitted in any VP of the VPN. Moreover, in case of congestion the traffic will be throttled as close to the sources as possible.

Although the invention has been described and illustrated with respect to a FR network, the present invention is equally applicable to other packet switching networks. For example, an asychronous transfer mode (ATM) network includes virtual circuits and virtual paths. As opposed to a FR network, a VP is an actual logical entity in an ATM network. The ATM packets in the ATM network may be provided with address information to uniquely identify a packet as belonging to a specific VPN in accordance with the present invention.

Although the invention has been described and illustrated with respect to exemplary embodiments thereof, it should be understood by those skilled in the art that the foregoing, and various other additions and omissions may be made therein and thereto without departing from the spirit and scope of the present invention.

We claim:

1. A packet-based network for providing virtual private networks, each virtual private network carrying traffic associated with a particular customer of the packet-based network, the traffic including packets for transmission via the packet-based network, the packet-based network comprising:

a plurality of network elements, each being interconnected to at least one other network element by a physical path;

a plurality of customer premises equipment, each being interconnected to a network element by a physical path;

at least one virtual path, each being a logical connection between two virtual path terminators;

at least one virtual circuit, each being a logical connection established between two virtual circuit terminators, wherein packets are transmitted by said virtual circuits between the virtual circuit terminators;

wherein the virtual private network includes a collection of packet-based network resources including respective network elements, customer premises equipment, virtual paths and corresponding virtual circuits, the collection of packet-based network resources making up the virtual private network providing a level of service to the traffic associated with the particular customer of the packet-based network which is independent of all other traffic on the packet-based network which is outside of the virtual private network's logical domain; and

identification means contained in the packets of a respective customer having a virtual private network for identifying the respective virtual circuits and virtual paths used by the virtual private network to which the packets are associated.

2. A packet-based network according to claim **1**, wherein said identification means is a local identifier of the respective virtual circuits and virtual paths used by the virtual private network, and wherein the packet-based network further includes means for updating said identification means during transmission of the packet of a respective customer within the packet-based network.

3. A packet-based network according to claim **1**, wherein:

each virtual path is made up of at least one virtual path segment which is a portion of a virtual path using a particular physical path; and

each virtual circuit is made up of at least one virtual circuit segment which is a portion of the virtual circuit carried by a virtual path between two adjacent network elements, between two adjacent customer premises equipment, or between adjacent network elements and customer premises equipment.

4. A packet-based network according to claim **3**, wherein virtual circuit and virtual path terminators include both network elements and customer premises equipment.

5. A packet-based network according to claim **1**, wherein said identification means includes an address field having a fixed length virtual circuit identifier field and a fixed length virtual path identifier field to uniquely identify the virtual circuit and virtual path over which the packet of information will travel.

6. A packet-based network according to claim **1**, wherein said identification means includes an address field made up of variable length subfields including a class type field, a virtual path identifier field and a virtual circuit identifier field to uniquely identify the virtual circuit and virtual path over which the packet of information will travel, said class type field identifying the length of the virtual path identifier field and virtual circuit identifier field.

7. A packet-based network according to claim **1**, wherein said identification means includes an address field in said

packets, said address field being an integrated field which identifies virtual paths and virtual circuits over which the packet of information will travel, said integrated field being encoded to uniquely identify how a frame of information is switched within said network elements.

8. A packet-based network according to claim 7, wherein each network element includes a connection table which identifies how a packet is routed within the network element based on the value of the integrated address field.

9. A packet-based network for providing virtual private networks, each virtual private network carrying traffic associated with a particular customer of the packet-based network, the traffic including packets for transmission via the packet-based network, the packet-based network comprising:

a plurality of network elements, each being interconnected to at least one other network element by a physical path:

a plurality of customer premises equipment, each being interconnected to a network element by a physical path;

at least one virtual path, each being a logical connection between two virtual path terminators;

at least one virtual circuit, each being a logical connection established between two virtual circuit terminators, wherein packets are transmitted by said virtual circuits between the virtual circuit terminators;

wherein the virtual private network includes a collection of packet-based network resources including respective network elements, customer premises equipment, virtual paths and corresponding virtual circuits;

identification means contained in the packets of a respective customer having a virtual private network for identifying the respective virtual circuits and virtual paths used by the virtual private network to which the packets are associated; and

wherein each virtual path on a physical path of the network is allocated a respective positive guaranteed bandwidth, and wherein when congestion occurs on a physical path, only a virtual path using bandwidth greater than the respective positive guaranteed bandwidth is required to reduce submission rate of packets onto the network.

10. A packet-based network according to claim 9, wherein the bandwidth utilization of each virtual path within the virtual private network is monitored, and wherein when one virtual path is utilizing less than its respective positive guaranteed bandwidth, any excess bandwidth is equally shared among the remaining virtu paths on a respective physical path in proportion to the respective positive guaranteed bandwidth of the remaining virtual paths with respect to a total bandwidth of the respective physical path.

11. A packet-based network according to claim 9, wherein each virtual circuit is provided with a virtual circuit bandwidth on a respective virtual path, and wherein even if the physical path utilized by a virtual circuit is congested, if the respective virtual path is lightly loaded, the virtual circuit can utilize bandwidth at least equal to or greater than its virtual circuit bandwidth.

12. A packet-based network for providing virtual private networks, each virtual private network carrying traffic associated with a particular customer of the packet-based network, the traffic including packets for transmission via the packet-based network, the packet-based network comprising:

a plurality of network elements, each being interconnected to at least one other network element by a physical path;

a plurality of customer premises equipment, each being interconnected to a network element by a physical path;

at least one virtual path, each being a logical connection between two virtual path terminators;

at least one virtual circuit, each being a logical connection established between two virtual circuit terminators, wherein packets are transmitted by said virtual circuits between the virtual circuit terminators;

wherein the virtual private network includes a collection of packet-based network resources including respective network elements, customer premises equipment, virtual paths and corresponding virtual circuits;

identification means contained in the packets of a respective customer having a virtual private network for identifying the respective virtual circuits and virtual paths used by the virtual private network to which the packets are associated; and

means for establishing a virtual path within the packet-based network locally at each network element traversed by the virtual path, said means for establishing a virtual path including:

means for identifying an outgoing physical path from a network element with available bandwidth to support a guaranteed bandwidth of the virtual path and able to support a number of virtual circuits carried by the virtual path;

means for reserving resources on the physical paths, the reserved resources being indicative of the virtual path bandwidth and number of virtual circuits carried by the virtual path; and

means for updating a connection table in the network element by mapping incoming virtual circuits and virtual paths to respective outgoing virtual circuits and virtual paths.

13. A packet-based network according to claim 12 further including means for establishing a virtual circuit within a virtual private network including:

means for identifying a respective virtual path towards a destination having at least the available bandwidth required by the virtual circuit and an unused virtual circuit segment;

means for reserving resources for the virtual circuit on the respective virtual path, the reserved resources for the virtual circuit being indicative of the virtual circuit bandwidth and the virtual circuit segment on the respective virtual path; and

means for updating the connection table within the network element.

14. A packet-based network according to claim 12, further including means for establishing a signalling virtual circuit on each virtual path.

15. A packet-based network for providing virtual private networks, each virtual private network carrying traffic associated with a particular customer of the packet-based network, the traffic including packets for transmission via the packet-based network, the packet-based network comprising:

a plurality of network elements, each being interconnected to at least one other network element by a physical path;

a plurality of customer premises equipment, each being interconnected to a network element by a physical path;

at least one virtual path, each being a logical connection between two virtual path terminators;

at least one virtual circuit, each being a logical connection established between two virtual circuit terminators,

wherein packets are transmitted by said virtual circuits between the virtual circuit terminators;

wherein the virtual private network includes a collection of packet-based network resources including respective network elements, customer premises equipment, virtual paths and corresponding virtual circuits;

identification means contained in the packets of a respective customer having a virtual private network for identifying the respective virtual circuits and virtual paths used by the virtual private network to which the packets are associated, and

a physical service access point for each respective physical path which multiplexes all packets to be transmitted on the respective physical path, the physical service access point including a physical path queue which is served at a physical path rate, the physical path queue being shared by all virtual paths multiplexed on to the respective physical path.

16. A packet-based network according to claim 15 wherein a physical path congestion threshold is determined based on the maximum amount of packets stored in the physical path queue and waiting for transmission on to the respective physical path, and wherein a congestion notification is provided to each of the virtual paths multiplexed onto the respective physical path in response to the length of the physical path queue exceeding the physical path congestion threshold.

17. A packet-based network according to claim 16 wherein said congestion notification includes an additional bit in each packet.

18. A packet-based network according to claim 16 wherein said congestion notification includes a signaling frame transmitted from the physical service access point to each of the virtual paths multiplexed on the physical service access point.

19. A packet-based network according to claim 16 wherein:

each of the virtual paths multiplexed onto the respective physical path is allocated a corresponding positive guaranteed bandwidth;

the sum of the positive guaranteed bandwidth for all of the virtual paths multiplexed onto the respective physical path is less than a total bandwidth of the respective physical path, and

in response to said physical path congestion notification, each virtual path multiplexed onto the respective physical path reduces the submission rate of packets to the physical path queue to a level no greater than the corresponding positive guaranteed bandwidth.

20. A packet-based network according to claim 16 further including a virtual path service access point for each respective virtual path which multiplexes all packets to be transmitted on the respective virtual path from virtual circuits, the virtual path service access point including a virtual path queue which is served at a virtual path rate, the virtual path queue having a congestion threshold indicative of a maximum allowed virtual path queue length, the virtual path service access point providing a virtual path congestion notification to the virtual circuits carried by the respective virtual path in response to the length of the virtual path queue exceeding the virtual path queue threshold.

21. A packet-based network according to claim 20 wherein:

each of the virtual circuits multiplexed onto the respective virtual path is allocated a corresponding virtual circuit bandwidth;

the sum of the virtual circuit bandwidth for all of the virtual circuits multiplexed onto the respective virtual path is less than a guaranteed bandwidth of the respective virtual path, and

in response to the virtual path congestion notification, each respective virtual circuit multiplexed onto the respective virtual path reduces the submission rate of packets to the virtual path queue.

22. A packet-based network according to claim 21, wherein in response to persistence of said virtual path congestion notification after the reduction of the submission rate by each respective virtual circuit, each respective virtual circuit incrementally reduces submission rate until said virtual path congestion notification is removed, the respective virtual circuit only reducing submission rate to a level no greater than the corresponding virtual circuit bandwidth.

23. A packet-based network for providing virtual private networks, each virtual private network carrying traffic associated with a particular customer of the packet-based network, the traffic including packets for transmission via the packet-based network, the packet-based network comprising:

a plurality of network elements, each being interconnected to at least one other network element by a physical path;

a plurality of customer premises equipment, each being interconnected to a network element by a physical path;

at least one virtual path, each being a logical connection between two virtual path terminators;

at least one virtual circuit, each being a logical connection established between two virtual circuit terminators, wherein packets are transmitted by said virtual circuits between the virtual circuit terminators;

wherein the virtual private network includes a collection of Racket-based network resources including respective network elements, customer premises equipment, virtual paths and corresponding virtual circuits;

identification means contained in the packets of a respective customer having a virtual private network for identifying the respective virtual circuits and virtual paths used by the virtual private network to which the packets are associated; and

wherein a pseudo virtual path is provided on each physical path to carry traffic not associated with a virtual private network.

24. A packet-based network according to claim 23, wherein each virtual path and the pseudo virtual path on a physical path of the network is allocated a respective positive guaranteed bandwidth, and wherein when congestion occurs on a physical path, only a virtual path or pseudo virtual path using bandwidth greater than the respective positive guaranteed bandwidth is required to reduce submission rate of packets onto the network.

25. A packet-based network according to claim 24, wherein the bandwidth utilization of each virtual path within the virtual private network is monitored, and wherein when one virtual path is utilizing less than its respective positive guaranteed bandwidth, any excess bandwidth is equally shared among the remaining virtual paths on a respective physical path in proportion to the respective positive guaranteed bandwidth of the remaining virtual paths with respect to a total bandwidth of the respective physical path.

26. A packet-based network according to claim 24, wherein each virtual circuit is provided with a virtual circuit bandwidth on a respective virtual path, and wherein even if the physical path utilized by a virtual circuit is congested, if

the respective virtual path is lightly loaded, the virtual circuit can utilize bandwidth at least equal to or greater than its virtual circuit bandwidth.

27. A packet-based network for providing virtual private networks, each virtual private network carrying traffic associated with a particular customer of the packet-based network, the traffic including packets for transmission via the packet-based network, the packet-based network comprising:

a plurality of network elements, each being interconnected to at least one other network element by a physical path;

a plurality of customer premises equipment, each being interconnected to a network element by a physical path;

at least one virtual path, each being a logical connection between two virtual path terminators;

at least one virtual circuit, each being a logical connection established between two virtual circuit terminators, wherein packets are transmitted by said virtual circuits between the virtual circuit terminators;

wherein the virtual private network includes a collection of packet-based network resources including respective network elements, customer premises equipment, virtual paths and corresponding virtual circuits,

identification means contained in the packets of a respective customer having a virtual private network for identifying the respective virtual circuits and virtual paths used by the virtual private network to which the packets are associated;

a general network control center (GNCC) for controlling the packet-based network;

at least one virtual private network control center (VNCC), each respective VNCC being associated with a corresponding virtual private network; and

mediation means located between the GNCC and each respective VNCC for enabling communications therebetween;

wherein for communication from the GNCC to the respective VNCC said mediation means filters messages received from the packet-based network to ensure that GNCC messages are properly formatted for the respective VNCC and passes to the respective VNCC only those messages which pertain to traffic of the corresponding virtual private network; and

wherein for communication from the respective VNCC to the GNCC said mediation means screens VNCC messages to ensure the VNCC messages are properly formatted for the GNCC and to ensure that the VNCC messages are restricted to the packet-based network resources assigned to the corresponding virtual private network.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 5,768,271

DATED : June 16, 1998

INVENTOR(S) : Seid et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

At column 21, in line 48, "virtu" should be --virtual--.

At column 23, in line 11, "associated," should be --associated;--.

At column 24, in line 36, "Racket" should be --packet--.

At column 25, in line 25, "circuits." should be --circuits;--.

Signed and Sealed this

First Day of September, 1998

Bruce Lehman

BRUCE LEHMAN

Commissioner of Patents and Trademarks

Attest:

Attesting Officer

US005757775A

United States Patent [19]

Yokoyama et al.

[11] Patent Number: 5,757,775

[45] Date of Patent: May 26, 1998

[54] **INTERFACE FOR DETECTING LOSS OF CALL SETUP ATM CELL TO PREVENT MISROUTING IN DESTINATION LOCAL NETWORK**

[75] Inventors: **Masaru Yokoyama**; **Hajime Kawamura**, both of Tokyo, Japan

[73] Assignee: **NEC Corporation**, Tokyo, Japan

[21] Appl. No.: **665,097**

[22] Filed: **Jun. 14, 1996**

[30] **Foreign Application Priority Data**

Jun. 14, 1995 [JP] Japan 7-146644

[51] **Int. Cl.**[6] **H04J 3/14**

[52] **U.S. Cl.** **370/242**; 370/474; 370/395

[58] **Field of Search** 370/242, 243, 370/244, 245, 250, 252, 241, 229, 230, 235, 216, 392, 394, 395, 396, 397, 398, 399, 410, 419, 420, 421, 422, 428, 463, 465, 471, 472, 473, 474, 475, 476, 522, 528, 525, 529, 389, 401, 402, 403, 404, 405, 246, 247, 469, 467; 340/825.06, 825.16, 825.17; 379/63

[56] **References Cited**

U.S. PATENT DOCUMENTS

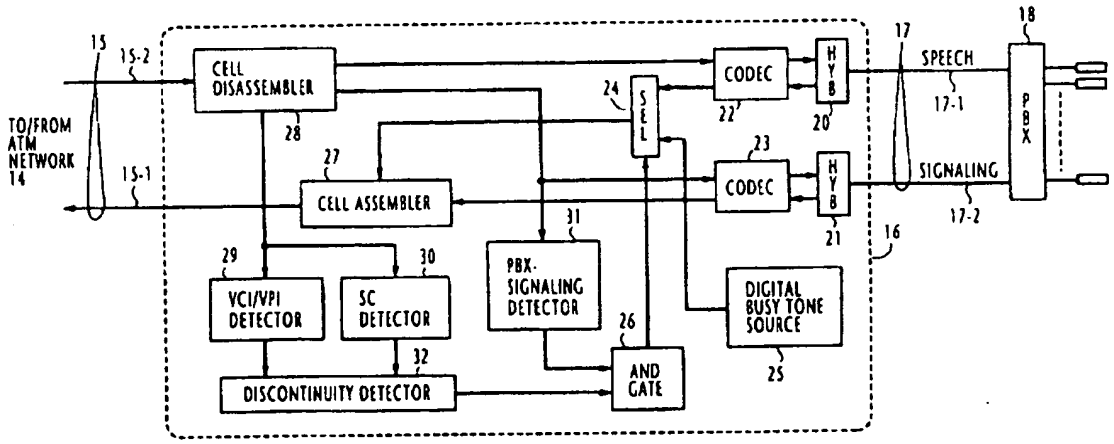
5,086,507	2/1992	Mela	379/63
5,101,403	3/1992	Balzano	370/242
5,459,722	10/1995	Sherif	370/474
5,461,607	10/1995	Miyagi et al.	370/244
5,553,057	9/1996	Nakayama	370/241

Primary Examiner—Wellington Chin
Assistant Examiner—Huy D. Vu
Attorney, Agent, or Firm—Sughrue, Mion, Zinn, Macpeak and Seas.

[57] **ABSTRACT**

An interface between an ATM network and a local network includes a cell disassembler for disassembling ATM cells from the ATM network and transmitting a disassembled signal to the local network. A cell assembler assembles a signal from the local network into ATM cells and transmitting the ATM cells to the ATM network. A cell loss detector is provided for detecting a loss of a cell in a series of ATM cells from the ATM network. A signaling cell detector detects a call setup ATM cell from the ATM network. A coincidence gate produces an output when there is a coincidence between the detection of the cell loss and the detection of the call setup ATM cell. When the coincidence is detected, a busy tone is supplied to the cell assembler, where it is assembled into ATM cells and transmitted to the ATM network.

6 Claims, 1 Drawing Sheet



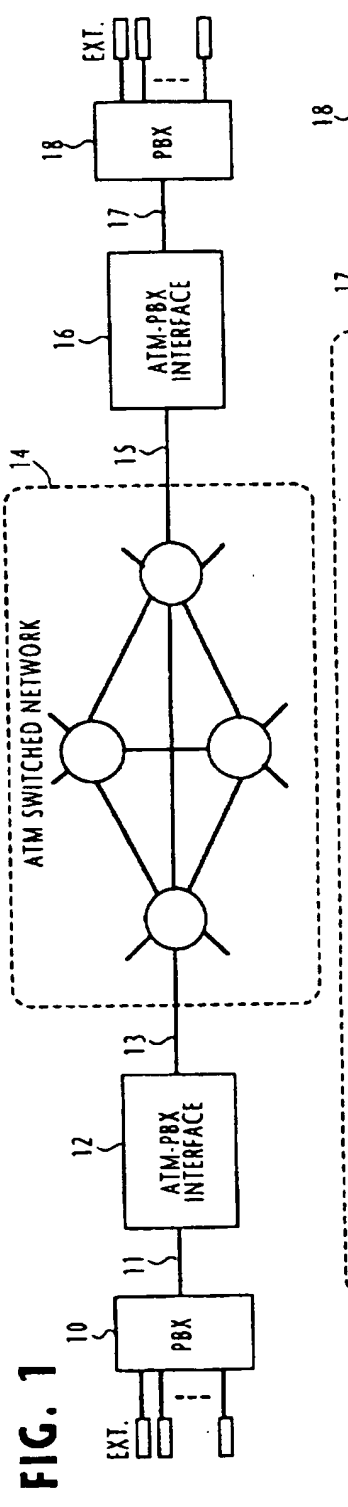


FIG. 1

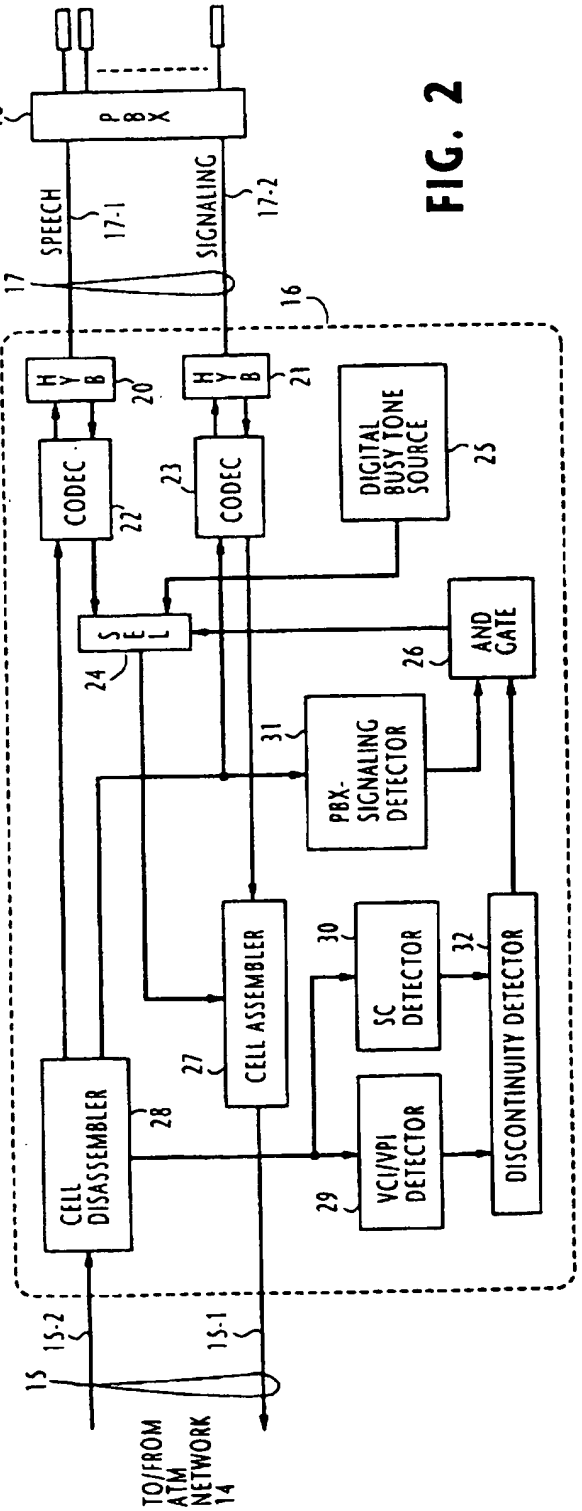


FIG. 2

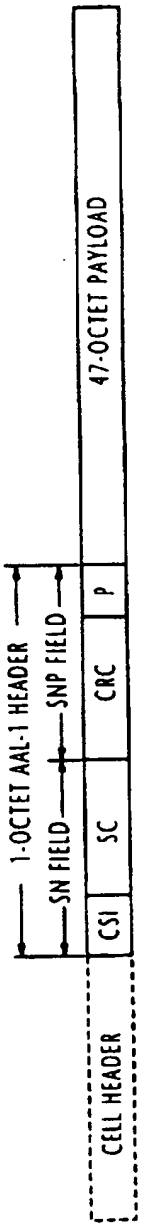


FIG. 3

cell header of a disassembled ATM cell and a 1-octet AAL-1 (ATM Adaptation Layer-1) header of the ATM cell, respectively. In addition, a PBX signaling detector **31** is connected to the signaling output port of disassembler **278** to produce an output signal when it detects a signaling cell for establishing a connection from PBX **10** to PBX **18**.

As shown in FIG. **3**, the AAL layer of ATM cell format according to the ITU-T Recommendations I-363 and I-365. 1 comprises a 5-octet cell header followed by a 48-octet information field. The first 1 octet of the information field is the AAL-1 header which contains a 4-bit serial number (SN) field and a 4-bit serial number protection (SNP) field. The SN field comprises a 1-bit convergence sublayer identifier (CSI) subfield and a 3-bit serial count (SC) subfield, and the SNP field comprises a 3-bit cyclic redundancy check (CRC) code subfield and a 1-bit parity bit (P).

The VCI/VPI detector **29** detects the VCI/VIP (virtual channel identifier/virtual path identifier) field of the cell header supplied from cell disassembler **28** and holds the VCI/VPI value in a memory so that a sequence of VCI/VPI values is stored. The SC detector **30** detects the serial count value in the AAL-1 header associated with the VCI/VPI value detected by detector **29** and holds the SC value in a memory so that a sequence of serial count values is stored. The sequences of VCI/VPI and serial count values are supplied from detectors **29** and **30** to a discontinuity detector **32**. Using the VCI/VPI values from detector **29**, the discontinuity detector **32** determines whether there is a discontinuity in the sequence of sequence count values of a particular VCI/VPI value.

If cell sequence integrity is maintained in the ATM network **14** for a connection from PBX **10** to PBX **18**, there is no loss of cells from the source network node and the sequence count values stored in the SC detector **30** at the destination ATM-PBX interface **16** vary consecutively from 0 to 7 and cyclically repeats the same consecutive values (i.e., a modulo 8). If there is a cell loss in the ATM network **14**, there is a discontinuity in the modulo-8 count values for a particular VCI/VPI value in SC detector **30** and the discontinuity detector **32** supplies an output signal to the coincidence gate **24**. If a cell loss event is detected at the same time a signaling cell is detected by PBX-signaling detector **31**, there is a coincidence at the inputs of the coincidence gate **24**. As a result, a switching command signal is produced by coincidence gate **26** and selector **24** is switched to the lower position for coupling the busy tone source **25** to the cell assembler **27**.

Therefore, ATM cells carrying a busy tone is transmitted through the network to the source ATM-PBX interface **12**. At the source interface **12**, these ATM cells are disassembled and converted to a busy tone signal and transmitted to the PBX **10**. The user at the call-originating terminal hears a busy tone and reattempts the call setup procedure. If the originating terminal is a fax machine, it responds to the busy tone by automatically reattempting the call setup procedure.

What is claimed is:

1. An interface between an asynchronous transfer mode (ATM) network and a local network, comprising:

a cell loss detector for detecting a cell loss in a series of ATM cells from the ATM network;

a signaling cell detector for detecting a call setup ATM cell from the ATM network;

a coincidence gate for detecting a coincidence between the detection of a cell loss by the cell loss detector and the detection of a call setup ATM cell by the signaling cell detector; and

means for assembling an audible tone into ATM cells and transmitting the ATM cells to the ATM network when said coincidence is detected.

2. An interface as claimed in claim **1**, wherein said audible tone is a busy tone.

3. An interface as claimed in claim **1**, wherein said cell loss detector comprises:

a VCI/VPI (virtual channel identifier/virtual path identifier) detector for detecting VCI/VPI values from ATM cells received from the ATM network;

a sequence count detector for detecting sequence count values from said ATM cells; and

a discontinuity detector connected to the VCI/VPI detector and the sequence count detector for detecting a cell loss when there is a discontinuity in the sequence count values detected by the sequence count detector for a particular VPI/VCI value detected by the VCI/VPI detector.

4. An interface between an asynchronous transfer mode (ATM) network and a local network, comprising:

a cell disassembler for disassembling ATM cells from the ATM network and transmitting a disassembled signal to the local network;

a cell assembler for assembling a signal from the local network into ATM cells and transmitting the ATM cells to the ATM network;

a cell loss detector for detecting a cell loss in a series of ATM cells from the ATM network;

a signaling cell detector for detecting a call setup ATM cell from the ATM network;

a coincidence gate for detecting a coincidence between the detection of a cell loss by the cell loss detector and the detection of a call setup ATM cell by the signaling cell detector; and

means for supplying an audible tone to the cell assembler when said coincidence is detected.

5. An interface as claimed in claim **4**, wherein said audible cone is a busy tone.

6. An interface as claimed in claim **4**, wherein said cell loss detector comprises:

a VCI/VPI (virtual channel identifier/virtual path identifier) detector for detecting VCI/VPI values from ATM cells received from the network;

a sequence count detector for detecting sequence count values from said ATM cells; and

a discontinuity detector connected to the VCI/VPI detector and the sequence count detector for detecting a cell loss when there is a discontinuity in the sequence count values detected by the sequence count detector for a particular VPI/VCI value detected by the VCI/VPI detector.

* * * * *

US005619500A

United States Patent [19]

Hiekali

[11] Patent Number: 5,619,500

[45] Date of Patent: Apr. 8, 1997

[54] ATM NETWORK INTERFACE

[75] Inventor: Nasser Hiekali, San Jose, Calif.

[73] Assignee: Digital Link Corporation, Sunnyvale, Calif.

[21] Appl. No.: 299,737

[22] Filed: Sep. 1, 1994

[51] Int. Cl.[6] H04L 12/56

[52] U.S. Cl. 370/414; 370/396; 370/401; 370/419

[58] Field of Search 370/94.1, 94.2, 370/85.6, 85.13, 58.2, 60, 60.1, 99

[56] References Cited

U.S. PATENT DOCUMENTS

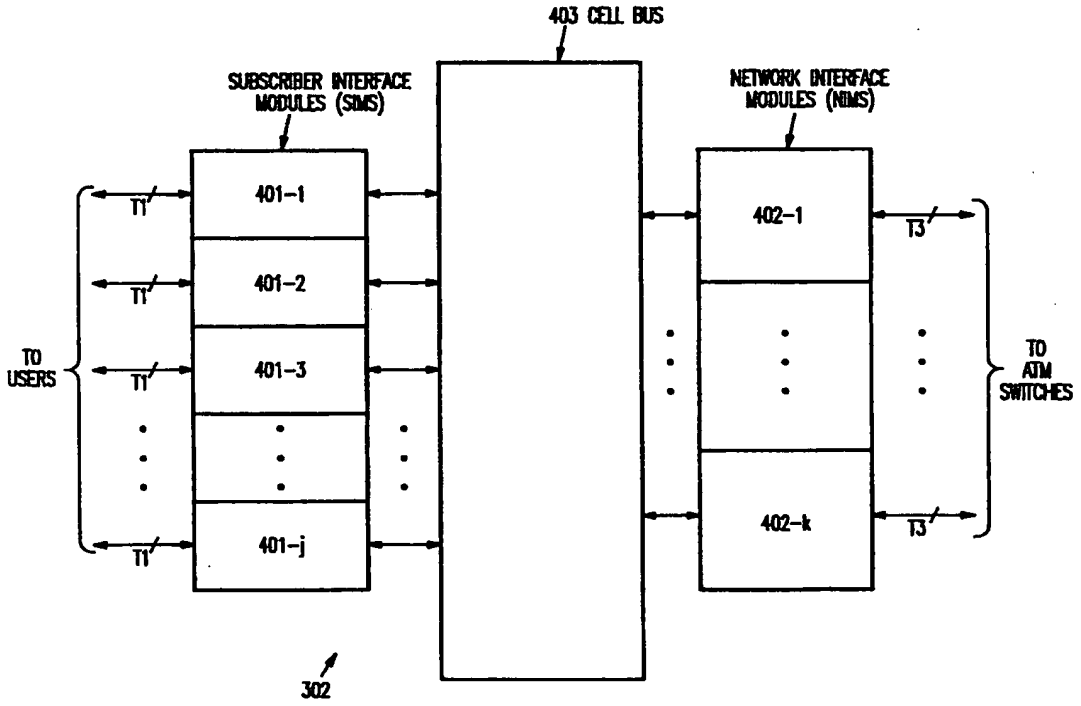
5,083,269	1/1992	Syobatake et al.	370/94.1
5,126,999	6/1992	Munter et al.	370/85.6
5,233,606	8/1993	Pashan et al.	370/85.6
5,278,828	1/1994	Chao	370/85.6
5,327,421	7/1994	Hiller et al.	370/94.2
5,357,506	10/1994	Sugawara	370/94.1

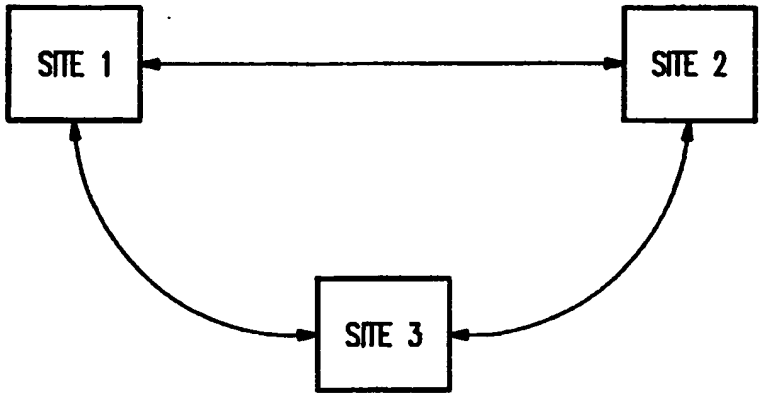
Primary Examiner—Douglas W. Olms
Assistant Examiner—Min Jung
Attorney, Agent, or Firm—Steven F. Caserza; Flehr, Hohbach, Test, Albritton & Herbert

[57] ABSTRACT

A novel ATM network provided which includes one or more ATM gateways for interfacing a plurality of T1 or fractional T1 signals with a higher bandwidth ATM network switch. In order to provide high speed and bandwidth utilizing relatively inexpensive and standard components, the data is stored in a memory, such as a video RAM, and pointers are utilized to indicate the type of each piece of data stored in the memory, including its priority for transmission to an ATM switch. In one embodiment of this invention, a plurality of pointer pools are used, each corresponding to a data type having a given priority. Pointers are placed into an appropriate one of the pools to define the order in which data will be transferred to the ATM switch in accordance with the priority of the data type and the receiving bandwidth of its destination in the ATM network. In one embodiment an HDLC controller is used which is suitable for framing a plurality of channels of data received on an incoming data path, such as a T1 channel. In order to minimize processing hardware requirements, a single HDLC controller is used to provide appropriate framing of each channel in a multiplexed fashion, with intermediate HDLC states being stored in a temporary state memory for retrieval when the next set of bits for a given channel is received for processing by the HDLC controller. A plurality of buffer memories are used for storing intermediate data corresponding to each of the incoming channels.

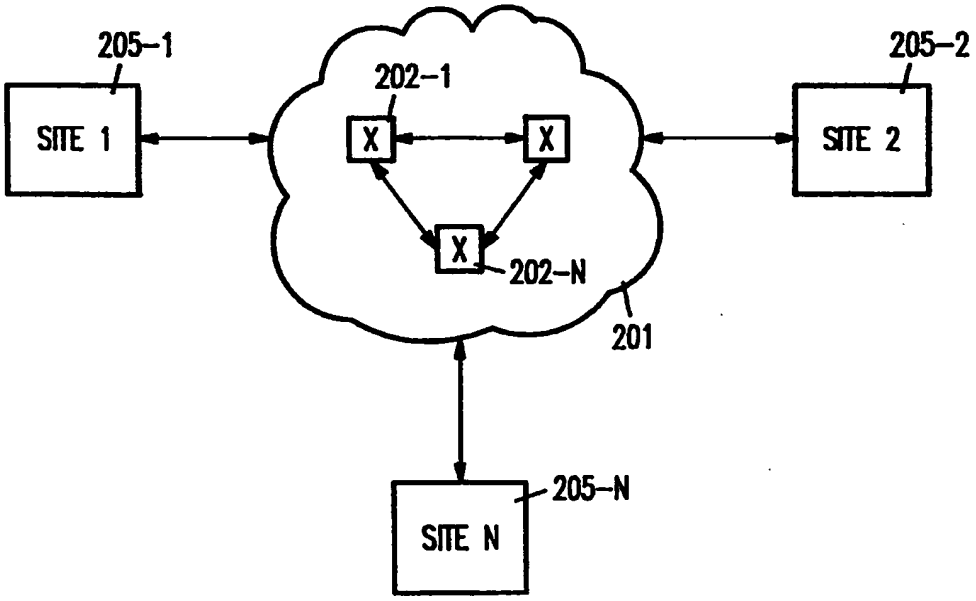
23 Claims, 10 Drawing Sheets





PRIOR ART

FIG. 1



PRIOR ART

FIG. 2

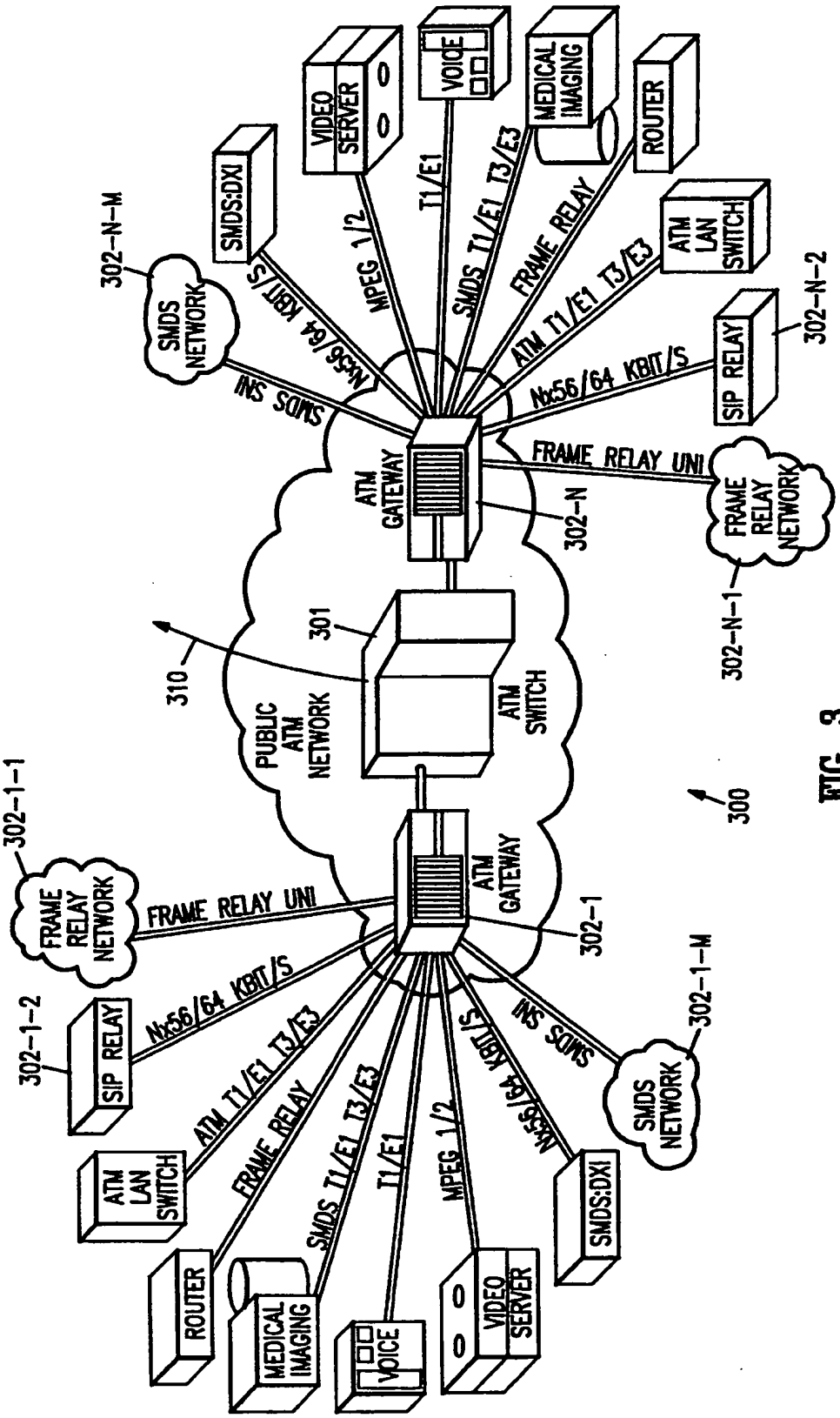

VIDEO SERVER
VOICE
MEDICAL IMAGING
ROUTER
SMDS:DXI
ATM LAN SWITCH
SIP RELAY
SMDS NETWORK
FRAME RELAY NETWORK
ATM GATEWAY
ATM SWITCH
PUBLIC ATM NETWORK
T1/E1
MPEG 1/2
SMDS T1/E1 T3/E3
FRAME RELAY
ATM T1/E1 T3/E3
Nx56/64 KBIT/S
FRAME RELAY UNI
INS SDMS
302-N-M
302-N
302-N-2
302-N-1
301
310
300
302-1
302-1-1
302-1-2
302-1-M

FIG. 3

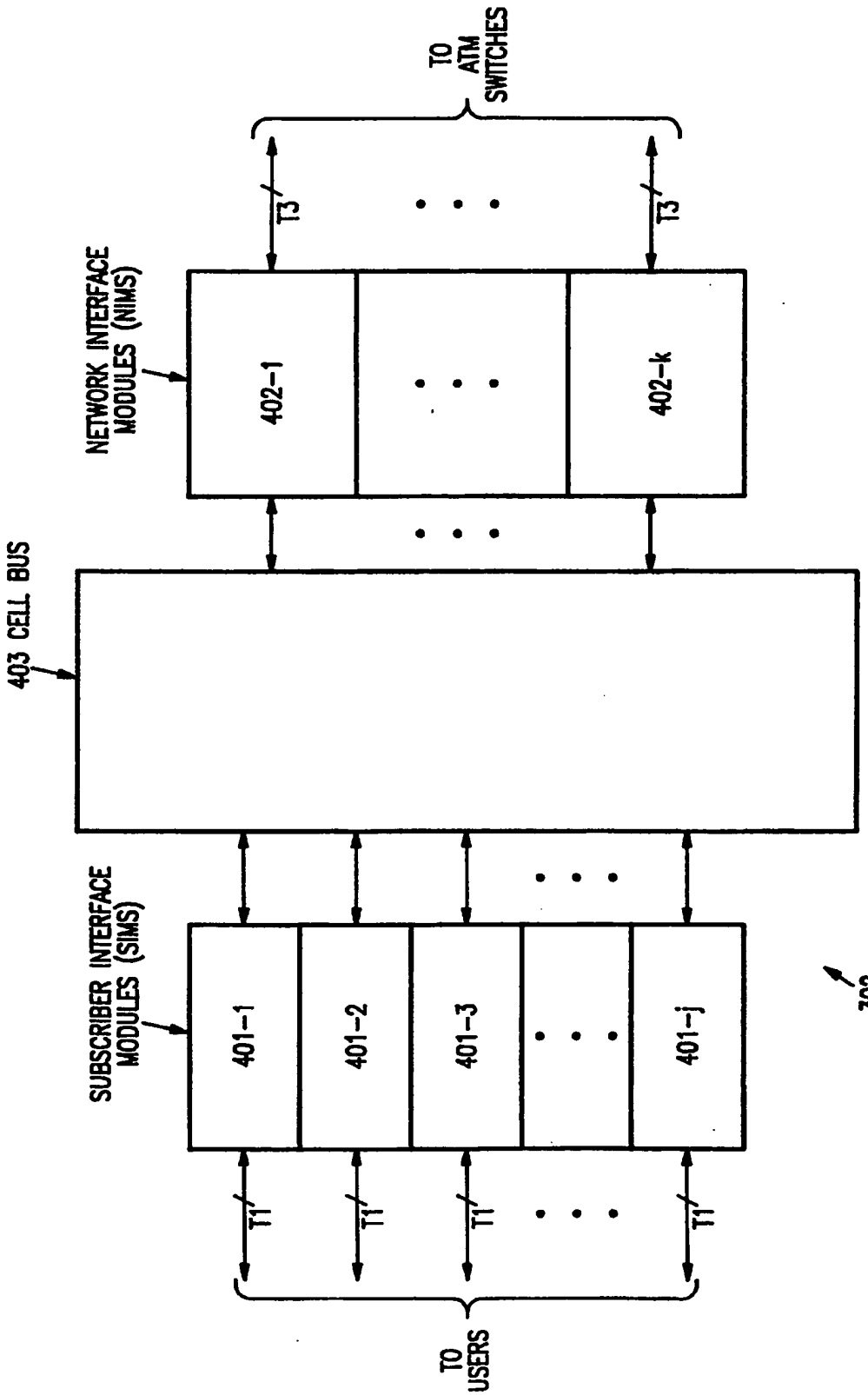

TO ATM SWITCHES
T3
T3
NETWORK INTERFACE MODULES (NIMS)
402-1
402-k
403 CELL BUS
SUBSCRIBER INTERFACE MODULES (SIMS)
401-1
401-2
401-3
401-j
T1
T1
T1
T1
TO USERS
302

FIG. 4

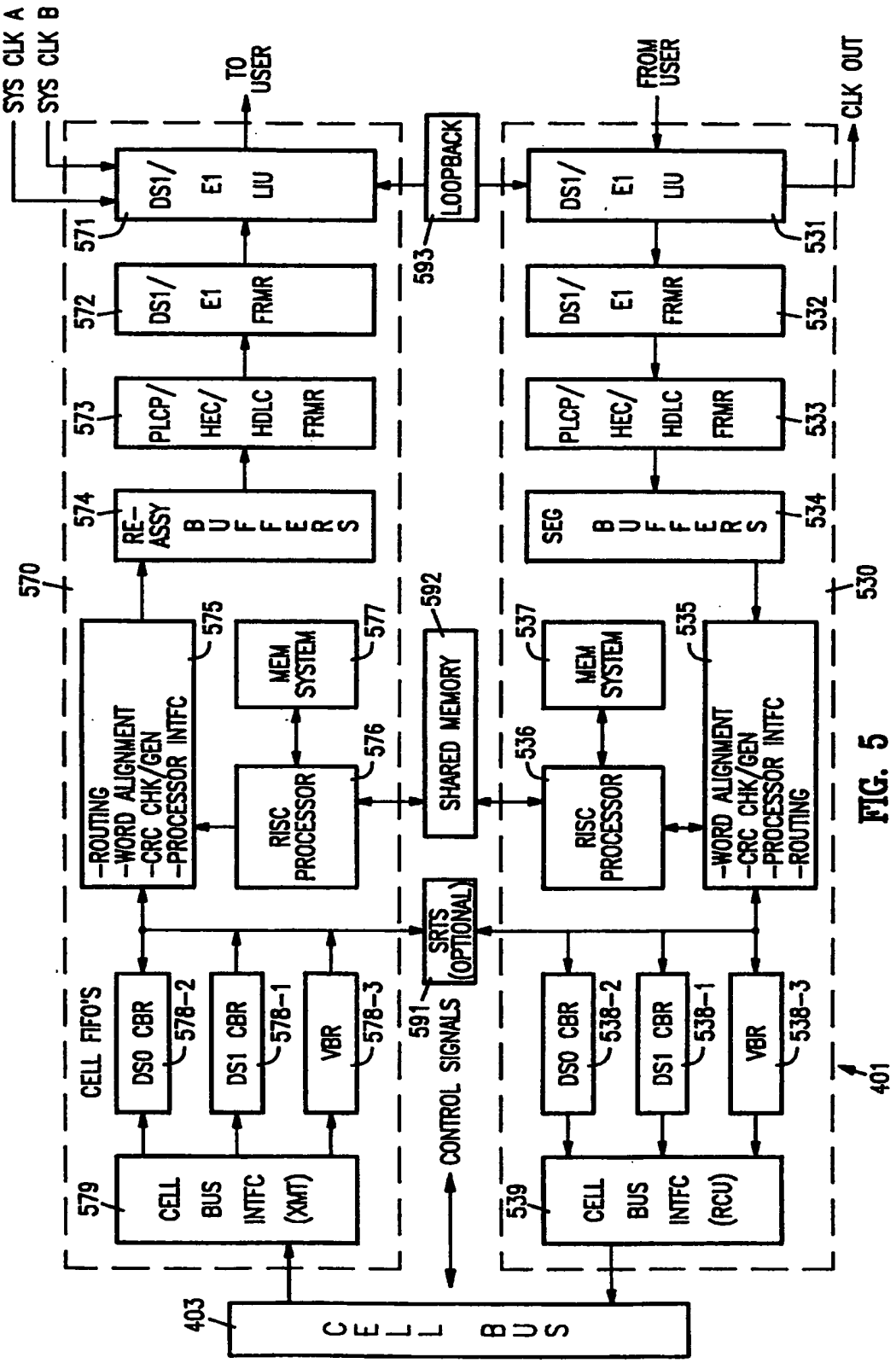

SYS CLK A
SYS CLK B
TO USER
FROM USER
CLK OUT
DS1/ E1 LIU
LOOPBACK
DS1/ E1 FRMR
PLCP/ HEC/ HDLC FRMR
RE-ASSY BUFFERS
SEG BUFFERS
-ROUTING -WORD ALIGNMENT -CRC CHK/GEN -PROCESSOR INTFC
MEM SYSTEM
RISC PROCESSOR
SHARED MEMORY
-WORD ALIGNMENT -CRC CHK/GEN -PROCESSOR INTFC -ROUTING
SRTS (OPTIONAL)
CELL FIFO'S
DS0 CBR
DS1 CBR
VBR
CONTROL SIGNALS
CELL BUS INTFC (XMT)
CELL BUS INTFC (RCU)
CELL BUS
570
571
572
573
574
575
576
577
592
593
530
531
532
533
534
535
536
537
578-2
578-1
578-3
591
538-2
538-1
538-3
579
539
403
401

FIG. 5

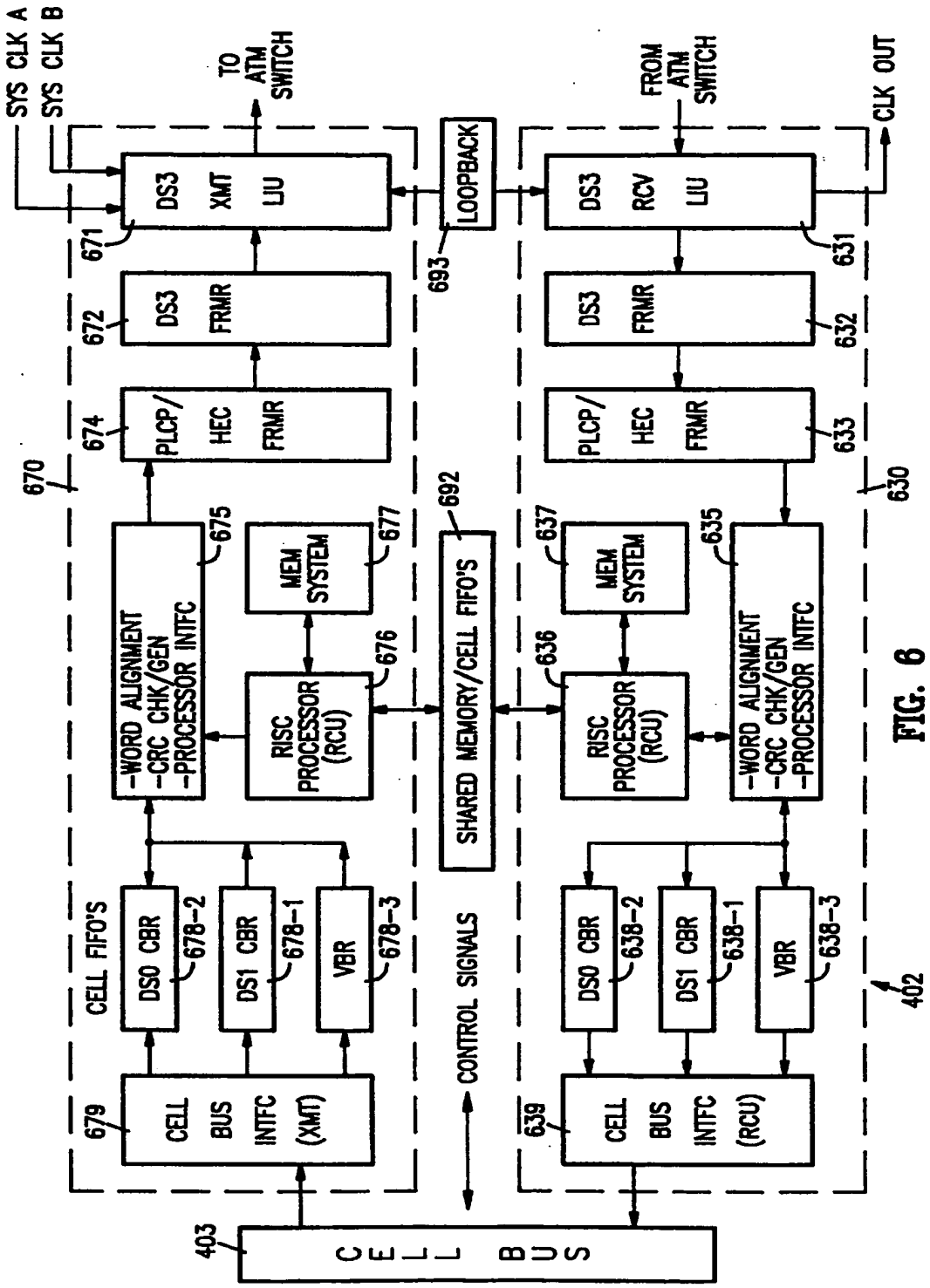

SYS CLK A
SYS CLK B
TO ATM SWITCH
FROM ATM SWITCH
CLK OUT
DS3 XMT LIU
671
LOOPBACK
693
DS3 RCV LIU
631
DS3 FRMR
672
DS3 FRMR
632
PLCP/ HEC FRMR
674
PLCP/ HEC FRMR
633
670
630
692
675
MEM SYSTEM
677
637
MEM SYSTEM
635
-WORD ALIGNMENT -CRC CHK/GEN -PROCESSOR INTFC
676
RISC PROCESSOR (RCU)
SHARED MEMORY/CELL FIFO'S
636
RISC PROCESSOR (RCU)
-WORD ALIGNMENT -CRC CHK/GEN -PROCESSOR INTFC
CELL FIFO'S
DS0 CBR
678-2
DS1 CBR
678-1
VBR
678-3
CONTROL SIGNALS
DS0 CBR
638-2
DS1 CBR
638-1
VBR
638-3
402
679
CELL BUS INTFC (XMT)
639
CELL BUS INTFC (RCU)
403
CELL BUS

FIG. 6

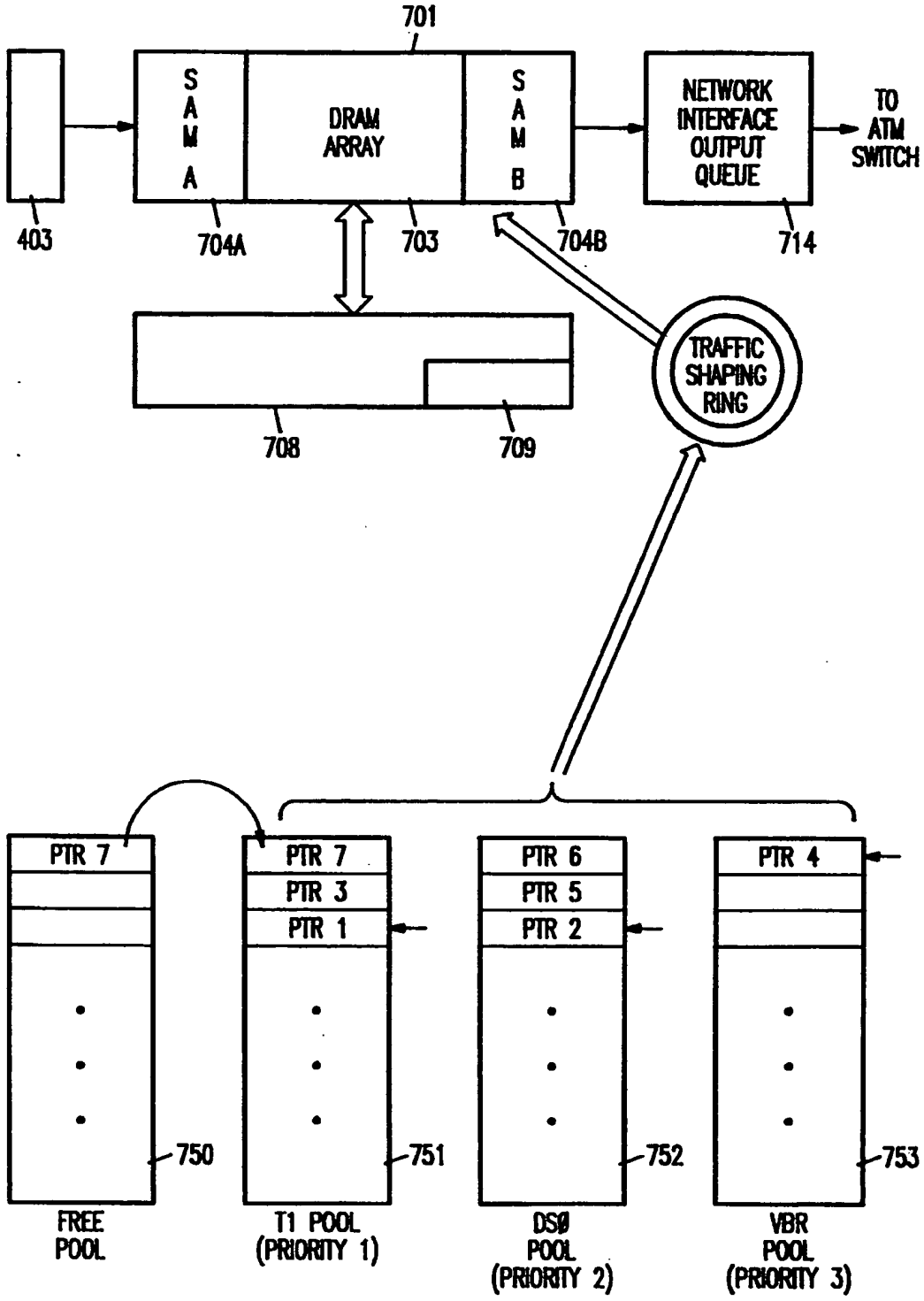

701
SAMA
DRAM ARRAY
SAMB
NETWORK INTERFACE OUTPUT QUEUE
TO ATM SWITCH
403
704A
703
704B
714
TRAFFIC SHAPING RING
708
709
PTR 7
PTR 7
PTR 3
PTR 1
PTR 6
PTR 5
PTR 2
PTR 4
750
751
752
753
FREE POOL
T1 POOL (PRIORITY 1)
DSØ POOL (PRIORITY 2)
VBR POOL (PRIORITY 3)

FIG. 7a

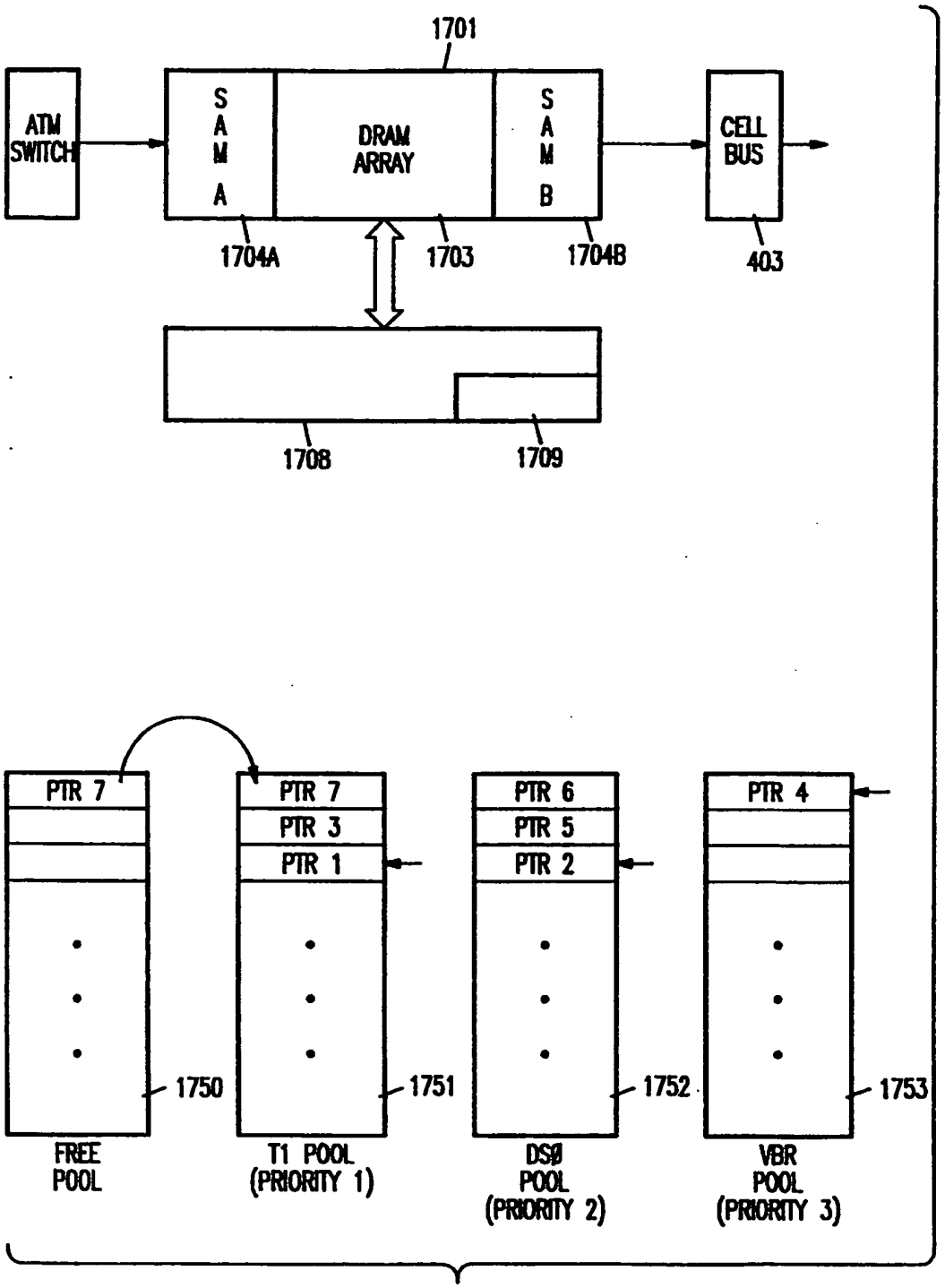

1701
ATM SWITCH
SAMA
DRAM ARRAY
SAMB
CELL BUS
1704A
1703
1704B
403
1708
1709
PTR 7
PTR 7
PTR 3
PTR 1
PTR 6
PTR 5
PTR 2
PTR 4
1750
1751
1752
1753
FREE POOL
T1 POOL (PRIORITY 1)
DSØ POOL (PRIORITY 2)
VBR POOL (PRIORITY 3)

FIG. 7b

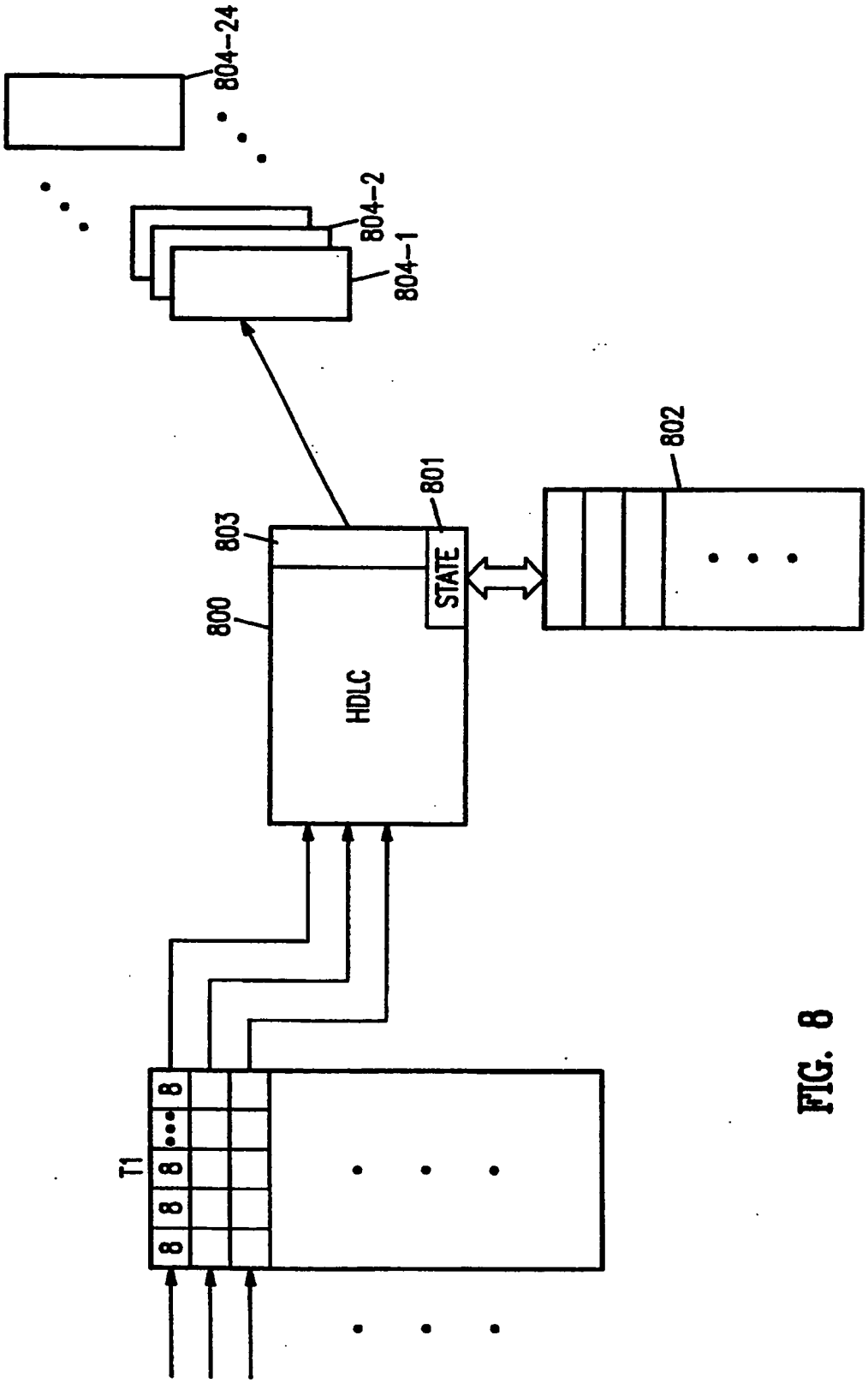


FIG. 8

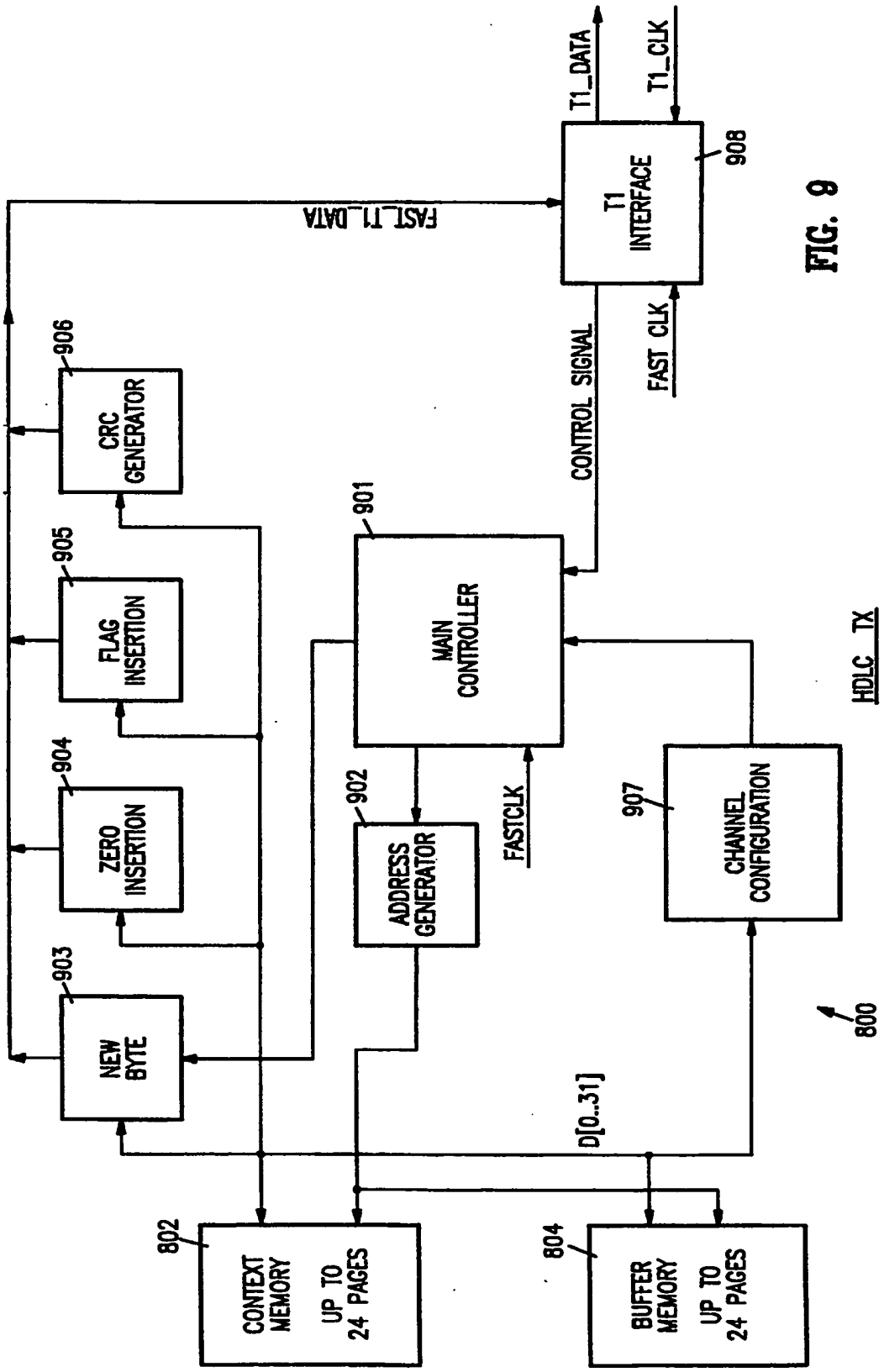

T1_DATA
T1_CLK
908
T1 INTERFACE
FAST_T1_DATA
906
CRC GENERATOR
CONTROL SIGNAL
FAST CLK
901
905
FLAG INSERTION
MAIN CONTROLLER
HDLC TX
904
ZERO INSERTION
902
ADDRESS GENERATOR
FASTCLK
907
CHANNEL CONFIGURATION
903
NEW BYTE
800
D[0..31]
802
CONTEXT MEMORY UP TO 24 PAGES
804
BUFFER MEMORY UP TO 24 PAGES

FIG. 9

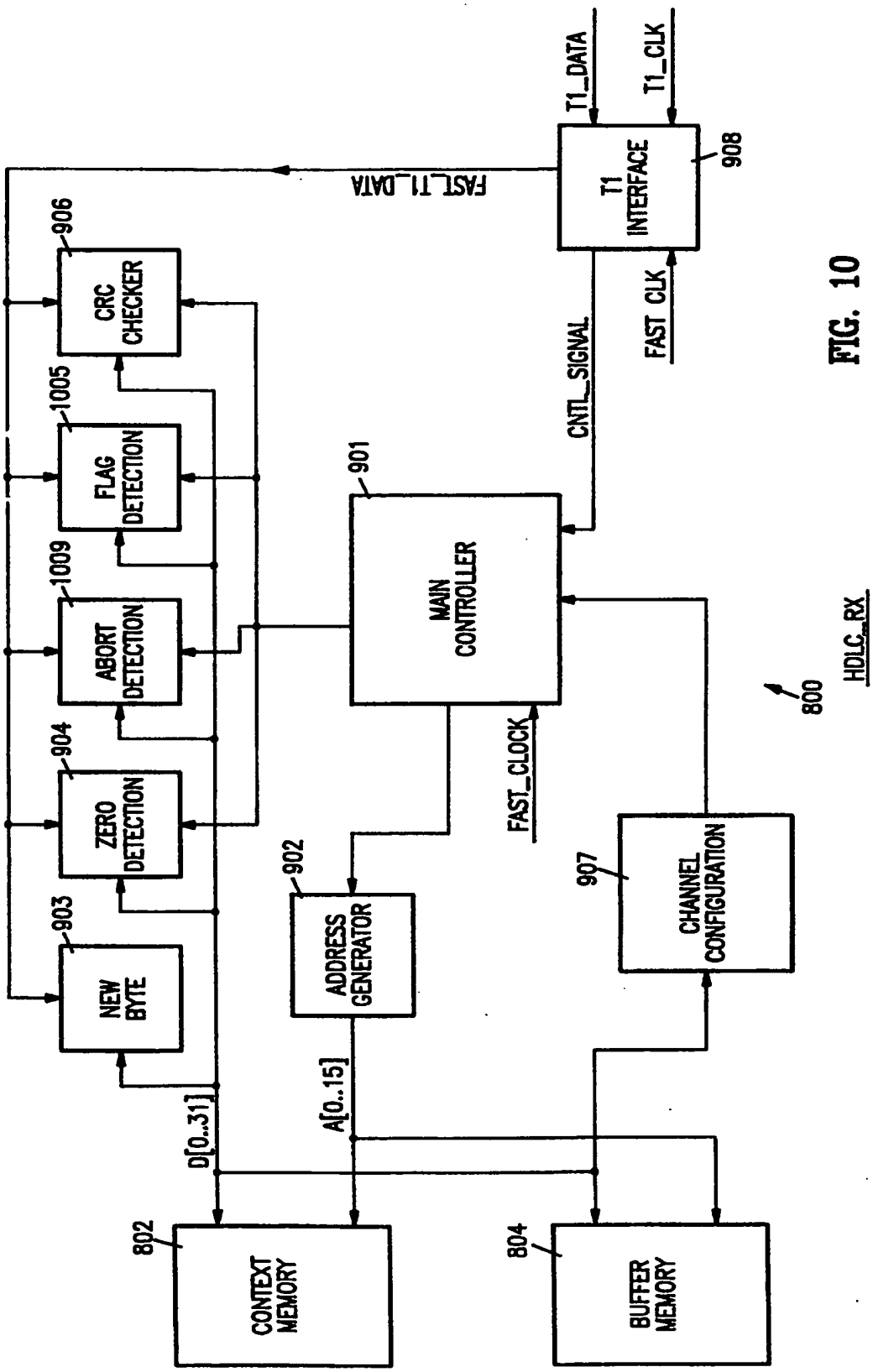

T1_DATA
T1_CLK
T1 INTERFACE
908
FAST_T1_DATA
906
CRC CHECKER
1005
FLAG DETECTION
1009
ABORT DETECTION
904
ZERO DETECTION
903
NEW BYTE
CNTL_SIGNAL
FAST CLK
901
MAIN CONTROLLER
FAST_CLOCK
902
ADDRESS GENERATOR
907
CHANNEL CONFIGURATION
800
HDLC_RX
D[0..31]
A[0..15]
802
CONTEXT MEMORY
804
BUFFER MEMORY

FIG. 10

ATM NETWORK INTERFACE

FIELD OF THE INVENTION

This invention pertains to telecommunication and more specifically to asynchronous transfer mode (ATM) networks and interfaces between such ATM networks and one or more types of access networks.

BACKGROUND

FIG. 1 is a diagram depicting a typical prior art telecommunications network, in which three site locations have a need for telecommunications therebetween. In the prior art, dedicated lines, such as single user phone lines, are leased and connected between each of the three sites. For greater bandwidth, these interconnecting leased lines may be T1 lines, which are equivalent to 24 single voice channels, or a data rate of 1.544 megabits/second, or T3 lines, having a bandwidth equivalent to a plurality of T1 lines, having a bandwidth of 44.736 megabits/second. Such lines are expensive to lease, and are somewhat clumsy when a user's needs vary or are significantly less than the full bandwidth provided by a T1 or T3 leased line, since the user must lease and pay for unneeded capacity. While reference is made in this application to T1 and T3 lines and capacities, it is understood that in other parts of the world E1 and E3 lines are the standards, with an E1 line having a capacity of 32 voice channels as compared with the 24 voice channels of the T1 standard.

While there exists prior art switches which allow the multiplexing of a plurality of fractional T1 bandwidth lines into a single T1 signal, a more modern approach is the use of an asynchronous transfer mode (ATM) network, as depicted in FIG. 2. FIG. 2 depicts a system including an ATM network **201** which includes a plurality of high bandwidth data switches **202-1** through **202-N**, and appropriate high speed links therebetween. Such links are typically T3 links at the present time. ATM network **201** is maintained by a long distance carrier company, such as AT&T or MCI, the local phone company, an international carrier, or private network. Individual users located at sites **205-1** through **205-N** connect into ATM network **201** at their local ATM network access points and share resources of the ATM network in order to communicate with a distant site. This sharing of ATM network resources provides for more economical telecommunications in that ATM network facilities are shared among a number of users in a time varying fashion to account for variation in individual site needs over time. The use of the ATM network also reduces the number of telecommunication lines, since a complete permutation of telecommunication lines between sites which must communicate with each other is no longer needed.

However, there remains a difficulty in the implementation of the ATM network in that there is a mismatch between the T3 minimum bandwidth access to switches **202-1** through **202-N** of ATM network **201**, and the T1 or fractional T1 bandwidth of a number of users seeking access to ATM network **201**. This difficulty is exacerbated by the fact that there exists a number of data communication standards which are commonly used and which are not compatible with a single T3 signal. Such existing widely used standards include the previously mentioned 24 voice channels multiplexed on a T1 carrier, frame relay protocol, switched multi-megabit data service (SMDS) interface protocol (SIP) relay formed from a plurality of 56k bit per second data channels, video signals (for example, MPEG standard), and the ATM protocol itself.

SUMMARY

According to the teachings of this invention, a novel ATM network is provided which includes one or more ATM gateways for interfacing a plurality of T1 or fractional T1 signals with a higher bandwidth ATM network switch. In order to provide high speed and bandwidth utilizing relatively inexpensive and standard components, the data is stored in a memory, such as a video RAM, and pointers are utilized to indicate the type of each piece of data stored in the memory, including its priority for transmission to an ATM switch. In one embodiment of this invention, a plurality of pointer pools are used, each corresponding to a data type having a given priority. Pointers are placed into an appropriate one of the pools to define the order in which data will be transferred to the ATM switch in accordance with the priority of the data type and the receiving bandwidth of its destination in the ATM network.

As a feature of this invention, in one embodiment an HDLC controller is used which is suitable for framing a plurality of channels of data received on an incoming data path, such as a T1 channel. In order to minimize processing hardware requirements, a single HDLC controller is used to provide appropriate framing of each channel in a multiplexed fashion, with intermediate HDLC states being stored on a temporary state memory for retrieval when the next set of bits for a given channel is received for processing by the HDLC controller. A plurality of buffer memories are used for storing intermediate data corresponding to each of the incoming channels.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a diagram depicting a typical prior art telecommunications network;

FIG. **2** is a diagram depicting a typical prior art ATM network;

FIG. **3** is a diagram depicting an ATM network including an ATM gateway constructed in accordance with the teachings of this invention;

FIG. **4** is a block diagram of a typical ATM gateway of the present invention;

FIG. **5** is a block diagram depicting one embodiment of a subscriber interface module **401** of FIG. **4**;

FIG. **6** is a block diagram depicting one embodiment of a network interface module **402** of FIG. **4**;

FIG. **7***a* is a diagram depicting a portion of memory system **677** of a network interface module of this invention;

FIG. **7***b* is a diagram depicting a portion of memory system **677** of a service interface module of this invention;

FIG. **8** is a diagram depicting one embodiment of an HDLC controller of this invention;

FIG. **9** is a block diagram depicting one embodiment of an HDLC transmit side circuitry corresponding to the HDLC controller of FIG. **8**; and

FIG. **10** is a block diagram depicting one embodiment of an HDLC receive side circuitry corresponding to the HDLC controller of FIG. **8**.

DESCRIPTION OF SPECIFIC EMBODIMENTS

In accordance with the teachings of this invention, an ATM gateway is provided to interface a plurality of T1 or

fractional T1 signals with a higher bandwidth ATM network switch.

FIG. 3 shows a diagram depicting such an ATM network 300 including an ATM switch 301, which is typically formed as a plurality of T3 circuits handling ATM protocol data over a wide service area. ATM network 300 also include a plurality of access ports such as access port 310 having the same bandwidth as the ATM network itself. In other words, for the typical current ATM networks formed of a plurality of switches of T3 bandwidth, a number of T3 access ports 310 are provided for users which need a T3 bandwidth access to ATM network. Also included in the ATM network 300 is a plurality of ATM gateways 302-1 through 302-N. Such ATM gateways include a plurality of ports for connection to a number of users utilizing any combination of a variety of standard protocols, such as a frame relay network user 302-1-1, SIP relay user 302-1-2, and the like. ATM gateway 302-1 interfaces between each of these sub T3 users, which require either T1 or fractional T1 bandwidths, and the ATM switch 301. ATM gateway 302-1 also provides any necessary translation between the various user protocols such as frame relay network, SIP relay, and the like, and the ATM protocol used by ATM network 300. ATM gateway 302-1 also provides local switching between these various sub T3 users, if desired.

FIG. 4 is a block diagram of a typical ATM gateway 302 of the present invention. ATM gateway 302 includes a plurality of service interface modules (SIMs) 401-1 through 401-j, each of which is capable of communicating to a user who via one or more T1 channels, such users utilizing any one or more of a number of well known protocols. ATM gateway 302 also includes one or more network interface modules (NIMs) 402-1 through 402-k, which interface to ATM switches via one or more wideband lines, associated with the T3 lines currently in widespread use, or in even wider bandwidth lies which will become more widely used in the future. SIMs 401-1 through 401-j are interfaced to NIMs 402-1 through 402-k, or to other SIMs (not shown), via cell bus 403 which is typically formed as a backplane bus into which a plurality of SIM cards and NIM cards are placed.

In one embodiment of this invention, by way of example only, an ATM gateway 302 is formed of nine SIMs, each of which can handle four input ports, each input port having a T1 bandwidth and thus capable of handling either a T1 signal or a fractional T1 signal, and a single NIM which handles two T3 connections to the ATM switch. In this embodiment, the ATM gateway also includes a management processor module (MPM) which for simplicity is not shown in FIG. 4, but which serves to provide configuration capability and storage, automatic fault diagnostics/isolation/recovery, and an external human interface. Also, in one such embodiment, ATM gateway 302 includes, under the control of the MPM, a spare SIM which can be hot swapped to replace a SIM which is diagnosed to have failed, as well as a spare NIM, which can be hot swapped in the event of a failure in one of the NIMs. If desired, ATM gateway 302 also includes a spare MPM for redundancy and therefore greater reliability.

FIG. 5 is a block diagram depicting one embodiment of a subscriber interface module (SIM) 401, previously described in FIG. 4. SIM 401 is an interface between a user, shown on the right side of FIG. 5, and cell bus 403. As previously mentioned, in one embodiment the users utilize sub T3 bandwidths, for example T1 or fractional T1 bandwidths, while cell bus 403 utilizes T3 or higher bandwidths for connection to the ATM switch. When a user sends data to the ATM network, it is received and processed by a RISC processor 536 and other related circuitry on input side 530 of SIM 401 and applied to cell bus 403. Conversely, when a user is to receive information from the ATM network, another RISC processor 576 and other related circuitry on cell bus side 570 of SIM 401 receives and processes information from the ATM network via cell bus 403 and provides it to the user with the appropriate bandwidth and data protocol.

When information is received from a user, it will be received in a non T3 ATM format. This data is received by line interface unit 531 which provides an appropriate electrical termination to a communications link from the user. Data is passed from line interface unit 531 to framer 532, which provides appropriate byte alignment framing of the received data in accordance with a DS1/E1 protocol. This framing is accomplished by monitoring incoming data and detecting framing signals, such as a predefined sequence of bits denoting the beginning and/or end of a data frame. In the event the user is providing a fractional T1 signal, only those channels assigned to that user would be used. SIM 401 utilizes the unused channels, and may fill those unused channels with another user's data, voice, video, or idle patterns.

The properly byte aligned framed data is provided by framer 532 to transmission convergence (Physical Layer Convergence Protocol (PLCP), High Level Data Link (HDLC), or Header Error Control (HEC)) framer 533, which serves to delineate the cells or frames contained in the incoming data. Data frames from framer 533 are provided in a parallel fashion to segmentation buffers 534 which serve to segment the frames into cells. If cells are contained in the incoming data, this function is bypassed. These parallel data cells are provided by segment buffers 534 to processing circuitry 535 which is controlled by microprocessor 536, which has access to memory system 537.

Processing circuitry 535 assists RISC processor 536, by performing a number of functions. First, circuitry 535 performs a word alignment function, which is needed to reduce the number of clock cycles used by processor 535 to align the incoming data to the proper format for processing. Circuitry 535 also performs an error detection and correction function, by generating a CRC on the incoming data and comparing that with a CRC stored as part of the incoming data. Circuitry 535 also performs a processor interfacing function, which serves to insure proper timing to and from the memory system 537, segmentation buffers 534 and circuits 538-1, 538-2 and 538-3. Circuitry 535 also provides the routing information necessary to direct the cells to proper destinations on cell bus 403. The resulting data from processor 535 is applied to one of a plurality of first-in-first-out (FIFO) circuits 538. In the embodiment shown in FIG. 5, three such FIFO circuits 538 are used for the following purposes. FIFO circuit 538-1 provides the highest priority queuing of cells to cell bus 403 of the received information from an entire T1 signal carrying 24 channels of voice/data information. FIFO circuit 538-2 is a buffer which serves to queue individual voice/data channel information, when received from a user with a DS0 data protocol. FIFO circuit 538-3 serves to queue variable bit rate data received from the user to cell bus 403. The output of each FIFO circuit 538-1 through 538-3 is applied to cell bus interface 539 for application to cell bus 403. Naturally, it will be appreciated that other types of FIFO circuits 538 can be employed in accordance with the teachings of this invention in addition to those shown in the exemplary embodiment of FIG. 5. Appropriate information is contained in the incom-

ing data stream from a user to define the type of data being received, allowing the routing function of processor circuit 535 to route received data to the appropriate one of the FIFO circuits 538.

The cell bus side 570 of subscriber interface module 401 operates in a corollary fashion. When information is received from the ATM switch, it is received in a standard ATM format. This data is received by cell bus interface unit 579 for application to FIFO circuits 578-1 through 578-3. FIFO circuits 578-1 through 578-3 correspond generally to FIFO circuits 538-1 through 538-3 of input side 530 of SIM 401. Output data from cell FIFO 578-1 through 578-3 is provided, in accordance with their priorities, to processing circuitry 575 which is assisted by RISC processor 576 to perform a number of functions. These functions are similar to those described previously with respect to input side 530, and include a word alignment function, CRC generation and checking, and a processor interfacing function. The resulting data is provided to reassembly buffers 574 which gathers cells to form the original frames/packet data. The output from reassembly buffers 574 is provided to framer 573 which serves to place the appropriate transmission convergence sublayer framing on the data. The resulting output from framer 573 is applied to framer 572 which serves to insert the appropriate DS1/E1 framing bits into the data. The output from framer 572 is fed to line interface unit 571, which provides an appropriate electrical interface to the user.

In one embodiment of this invention, subscriber interface module 401 includes a loop back circuit 593, which allows for testing of the user's communication link through line interface units 531 and 571, to determine if that portion of the network is operating properly. This feature is helpful for monitoring the condition of the line between subscriber interface module 401 and the user, and help determine when a malfunction is caused by subscriber interface module 401.

Shared memory 592 serves to provide a communications path between RISC processors 536 and 576. Status, configuration and test information is passed between the processors to ensure protocol balancing and proper handling of fault conditions.

In one embodiment, subscriber interface module 401 includes Synchronous Residual Time Stamp (SRTS) which serves to ensure information rate synchronization of the T1 signal utilizing the circuit emulation protocols.

FIG. 6 is a block diagram depicting one embodiment of a network interface module (NIM) 402, previously described in FIG. 4. NIM 402 is an interface between call bus 403, shown on the left side of FIG. 6, and an ATM switch. When the ATM network sends data for a user, it is received and processed by a RISC processor 636 and other related circuitry on input side 630 of NIM 402 and applied to cell bus 403. Conversely, when a user sends information for the ATM network, another RISC processor 676 and other related circuitry on the access side 670 of NIM 402 receives and processes information from cell bus 403 and provides it to the ATM with the appropriate bandwidth and data protocol.

When information is received from the ATM switch, it is received in an ATM format. This data is received by line interface unit 631 which provides an appropriate electrical termination to a communications link from the ATM switch. Data is passed from line interface unit 631 to framer 632, which provides appropriate byte/nibble alignment framing of the received data in accordance with a DS3/E3 protocol. This framing is accomplished by monitoring incoming data and detecting framing signals, such as a predefined sequence of bits denoting the beginning and/or end of a data frame.

The properly byte/nibble aligned framed data is provided by framer 632 to transmission convergence (PLCP or HEC) framer 633, which serves to delineate the cells contained in the incoming data. Data cells from framer 633 are provided in a parallel fashion to processing circuitry 635 which is controlled by microprocessor 636, which has access to memory system 637.

Processing circuitry 635 assists RISC processor 636, by performing a number of functions. First circuitry 635 performs an error detection and correction function, by generating a CRC on the incoming data and comparing that with a CRC stored as part of the incoming data. Circuitry 635 also performs a processor interfacing function, which serves to insure proper timing to and from the memory system 637, and framer 633, and circuits 638-1, 638-2 and 638-3. The resulting data from processor 635 is applied to one of a plurality of first-in-first-out (FIFO) circuits 638. In the embodiment shown in FIG. 6, three such FIFO circuits 638 are used for the following purposes. FIFO circuit 638-1 provides the highest priority queuing of cells to cell bus 403 of the received information from an entire T1 signal carrying 24 channels of voice/data information. FIFO circuit 638-2 is a buffer which serves to queue individual voice/data channel information, when received from a user with a DS0 data protocol. FIFO circuit 638-3 serves to queue variable bit rate data received from the ATM network to cell bus 403. The output of each FIFO circuit 638-1 through 638-3 is applied to cell bus interface 639 for application to cell bus 403. Naturally, it will be appreciated that other types of FIFO circuits 638 can be employed in accordance with the teachings of this invention in addition to those shown in the exemplary embodiment of FIG. 6. Appropriate information is contained in the incoming data stream from the ATM network to define the type of data being received, allowing the routing function of processor circuit 635 to route received data to the appropriate one of the FIFO circuits 638.

The cell bus side 670 of network interface module 402 operates in a corollary fashion. When information is received from the user vis cell bus 403, it is not received in a standard ATM format. This data is received by cell bus interface unit 679 for application to FIFO circuits 678-1 through 678-3. FIFO circuits 678-1 through 678-3 correspond generally to FIFO circuits 638-1 through 638-3 of input side 630 of NIM 402. Output data from cell FIFO 678-1 through 678-3 is provided, in accordance with their priorities, to processing circuitry 675 which is assisted by RISC processor 676 to perform a number of functions. These functions are similar to those described previously with respect to input side 630, and include a word alignment function, CRC generation and checking, and a processor interfacing function. The resulting data is provided to framer 674 which serves to place the appropriate transmission convergence (PLCP or HEC) sublayer on the outgoing cells. The output from framer 674 is provided to framer 672 which serves to insert the appropriate DS3/E3 framing bits into the data. The output from framer 672 is fed to line interface unit 671, which provides an appropriate electrical interface to the ATM switch.

During the operation of network interface module 402, when data is to be sent to the ATM switch after being received from a user (via the subscriber interface module 401 and cell bus 403), it is important that traffic shaping be provided. Traffic shaping serves to ensure that data is not sent to the ATM switch at a rate faster than the receiving station, connected to ATM switch at a distant location, can receive it. It also ensures that the data accumulating at any intermediate ATM switches does not exceed the switching

and buffering capacity of that ATM switch. For this reason, the ATM protocol requires ATM packets to include a connection ID indicating that this packet is part of a data connection between two specific ATM nodes. The connection ID contained within each ATM packet includes a virtual path ID (VPI) and a virtual connection ID (VCI). The VPI/VCI information is established in advance, based on the specific stations which are to communicate these packets, and the data rates capable by each of those stations. These data rates are defined to include both the average data rate and a peak data rate, and data rate shaping may be necessary to ensure that data is transferred in an efficient manner. For example, for proper data rate shaping, it is important to know whether data between two stations will be sent in rather constant bursts, or in high volume bursts sent rather infrequently.

All of this information goes into a database so that the database can be accessed based on the VPI/VCI information to determine data rate information. This data rate information indicates how fast data should be sent by network interface module **402** to the ATM switch, as a function of the data rate of the receiving station and intermediate ATM switches. Furthermore, it is typical that different types of data have different priorities. For example, it is normally expected that voice data has the highest priority, since voice data indicates that people are carrying on a conversation in real time and packets containing voice information should not be unduly delayed. On the other hand, computer information contained in data packets can be delayed somewhat without a significant single channel voice/data problem. Thus, it is common for 24 channels of voice/data to have priority **1**, (DS0) to have priority **2**, and variable bit rate data to have priority **3**.

Thus, when cell bus side **670** of network interface module **402** handles data received from the cell bus **403**, processor circuit **676** performs these prioritization and traffic shaping functions. Data cells are analyzed to determine their priority and, using the VPI/VCI look-up table, the data rate associated with their receiving station. Based on this information, information cells are moved to a traffic shaping ring at appropriate locations on that ring so that these data cells are output to the ATM switch in an appropriate sequence, with higher priority data cells being generally transmitted prior to lower priority data cells, and the transmission of data cells to a given destination, regardless of their priority, being transmitted so as not to exceed the data rate of the receiving station or intermediate ATM switches.

Due to the large amounts of data which are received by network interface module **402** from cell bus **403**, which must be manipulated and properly placed on the traffic shaping ring for later extraction and placement in a traffic queue prior to being sent to the ATM switch, a significant bandwidth is necessary for this activity. Thus, traffic shaping rings are typically formed from large amounts of static random access memory (SRAM) operating at high speed and consuming significant power, as is the output queue. The manipulation of this information is performed by custom designed integrated circuits operating as high speed state machines in order to provide the high speed processing required to handle the significant amounts of data being received from cell bus **403**. Thus, a significant expense is incurred in designing such processors, and their manufacturing cost is relatively high due to the rather small volume of components which are fabricated. Furthermore, the use of high speed SRAM in large quantities for the traffic shaping ring and output queue is expensive, and consumes a large amount of space and power.

In accordance with the teachings of this invention, a novel network interface module **402** is taught in which a portion of memory system **677**, configured as shown in FIG. **7***a*, is formed as a simple, relatively low speed/low power memory, thereby having significant reductions in cost, power consumption, and physical space requirements. In accordance with this invention, this memory is controlled using, for example, standard off the shelf microprocessors which are programmed to provide the necessary operating function, and without the requirement for a custom design high speed state machine device with its significantly increased cost. Cell data is received and stored in the low cost memory at an available location and the contents of each memory location is monitored by a series of pointer stacks or "pools".

One embodiment of this feature of the present invention is shown in FIG. **7***a*, in which cell bus **403** provides cell data to memory device **701** which comprises, for example, a video RAM of well known device and which is readily available from a number of vendors. A video RAM such as video RAM **701** includes a standard DRAM array **703** and an input serial access memory (SAM) **704***a*, and an output serial access memory **704***b*. Cell bus **403** provides serial data cells to VRAM **701**, which are serially loaded into SAM **704***a*. VRAM controller **708** is notified when bits are ready to enter SAM**704***a*. The VRAM controller finds an available location in the VRAM by "popping" the stack of free pool **750** which contains a set of pointers of unused locations in DRAM array **703**. It then programs the SAM and VRAM with this pointer. VRAM controller **708** then counts the number of bits serially entering SAM **704***a* in order to delineate a cell boundary, indicating when all bits of the data cell have been serially loaded into SAM **704***a*. At this time, VRAM controller **708** causes bits stored in SAM **704***a* to be transferred in parallel to an available location in DRAM **703** of VRAM **701**. Based on the type of data contained in the cell which has been received by SAM **704***a* for transfer to DRAM array **703**, the pointer from free pool **750** is transferred to one of a plurality of pools indicating the priority of cell data stored in DRAM array and the order in which those cells of various priorities have been placed into DRAM array **703**. In the embodiment of FIG. **7***a*, these pools are T1 pool **751**, DS0 pool **752**, and VBR pool **753**. As previously described, these pools are typically assigned priorities **1**, **2**, and **3**, respectively. Appropriate addressing techniques are used to indicate within a given one of these pools **751** through **753** which pointer should be used next to transfer cell information from DRAM array **703** to serial access memory **704***b* for transfer to network interface output queue **714**, which is then transferred out to the ATM switch.

In the example shown in FIG. **7***a*, with the various pointer information stored in the pools as shown in FIG. **7***a*, cell data will be transferred from DRAM **703** to network interface output queue **704** in the following sequence: PTR1, PTR3, PTR7, PTR2, PTR5, PTR7, and PTR4. Of course, it is likely that additional cell data will be received from cell bus **403** for storage in DRAM array **703** before this sequence of cell data transfer from DRAM array **703** is accomplished. In this event, additional pointers will be loaded into various ones of pools **751** through **753**, and the above sequence of transfer of cell data from DRAM array **703** will be altered due to the additional pointers stored in the pools.

When each cell of data is ready for transfer from DRAM array **703** to SAM **704***b*, a pointer is removed from the appropriate one of pools **751** through **753** and is used to program the VRAM, then it is placed back into free pool **750**. This indicates that that cell location within Dram array

703 is once again available for storage of an incoming cell of data received from cell bus 403. In operation under the control of a microprocessor (not shown), when SAM 704*b* is available following a transfer of its contents to network interface output queue 714, the microprocessor causes a transfer of the currently indexed pointer from the highest priority non-empty queue formed by pools 751 through 753. The microprocessor evaluates the VPI/VCI information contained in the data stored in the cell of DRAM array 703 pointed to by that transferred pointer in order to determine the necessary data rate shaping necessary for that cell of information. The microprocessor does this by looking at the database look-up table, using the VPI/VCI of the pointed to cell as a key and information stored in the database portion of the memory system indicating when the last cell of data was sent to the same destination. Based on this information, the microprocessor causes the pointer to be placed in the appropriate location on the traffic shaping ring. During the indexing of the traffic shaping ring, when a given location in the traffic shaping ring is reached, the contents of that location is a pointer which has been moved from the appropriate one of pools 751 through 753, and thus indicates the location within DRAM array 703 of the cell data which is to be moved to the output queue. The microprocessor uses this pointer which has been read from the traffic shaping ring to cause that cell of data to be transferred from DRAM array 703 to SAM704*b*, which information is then serially moved from SAM 704*b* to the ATM switch.

Thus, in accordance with the teachings of this invention, the significant amount of data forming the data cells is read from cell bus 403 serially into SAM 704*a*, transferred in parallel fashion to DRAM array 703, and later transferred to SAM 704*b* for serial transmission to the ATM switch. During this time, there is very little manipulation of the cell data itself since it is simply stored in video RAM 701. However, in accordance with the teachings of this invention, a significant amount of manipulation is performed utilizing a standard microprocessor and a series of pointer pools indicating the location of various data cells within video RAM 701. It is these pointers which are stored on the traffic shaping ring, which is later used to output the actual cell data from video RAM 701 to the ATM switch. Thus, in accordance with the teachings of this invention, a relatively slow (as compared with high power/high cost SRAM) video RAM is used to store cell information, and the variety of manipulations to determine pointer information is achieved quickly since pointers are relatively short (typically 16 bits, as compared with a typical cell size of 424 bits). In one embodiment of this invention, approximately 32 clock ticks are required to parallel load cell data into SAM 704*a*, 3 to 4 clock ticks are required to transfer the cell data from SAM 704*a* to DRAM array 703, and approximately 3 to 4 clock ticks are required to move cell data from DRAM array 703 to SAM 704*b*. In one embodiment, the pools are implemented using the same technology as that typically utilized in SRAM. Therefore, the time to manipulate a 16 bit pointer is the same as manipulating 16 bits of SRAM data. But since the amount of pool is significantly less than that normally needed to implement this function in SRAM, significant cost, power and board space reductions are achieved in accordance with this invention.

DRAM controller 708 also provides the necessary DRAM refresh cycles necessary to maintain the storage of its data.

Arbiter 709 ensures that accesses to the DRAM from the RISC processor and the VRAM circuitry that accesses the DRAM is achieved without interfering with each other's accesses. It grants access to the DRAM on a first-come-first-serve basis. However, in the event of a simultaneous access it will favor the DRAM controller.

In accordance with the teachings of this invention, a novel interface module 402 (FIG. 6) is taught in which a portion of memory system 637, configured as shown in FIG. 7*b*, is formed as a simple, relatively low speed/low power memory, thereby having significant reductions in cost, power consumption, and physical space requirements. In accordance with this invention, this memory is controlled using, for example, standard off the shelf microprocessors which are programmed to provide the necessary operating function, and without the requirement for a custom design high speed state machine device with its significantly increased cost. Cell data is received and stored in the low cost memory at an available location and the contents of each memory location is monitored by a series of pointer stacks or "pools".

One embodiment of this feature of the present invention is shown in FIG. 7*b*, in which the ATM switch provides cell data to memory device 1701 which comprises, for example, a video RAM of well known device and which is readily available from a number of vendors. A video RAM such as video RAM 1701 includes a standard DRAM array 1703 and an input serial access memory (SAM) 1704*a*, and an output serial access memory 1704*b*. The ATM switch provides serial data cells to VRAM 1701, which are serially loaded into SAM 1704*a*. VRAM controller 1708 is notified when bits begin to enter SAM 1704*a*, and VRAM controller 1708 then counts the number of bits serially entering SAM 1704*a* in order to delineate a cell boundary, indicating when all bits of the data cell have been serial loaded into SAM 1704*a*. At this time, VRAM controller 1708 causes bits stored in SAM 1704*a* to be transferred in parallel to an available location in DRAM 1703 of VRAM 1701. The available location is determined by "popping" the stack of free pool 1750 which contains a set of pointers of unused locations in DRAM array 1703. Based on the type of data contained in the cell which has been received by SAM 1704*a* for transfer to DRAM array 1703, the pointer from free pool 1750 is transferred to one of a plurality of pools indicating the priority of cell data stored in DRAM array and the order in which those cells of various priorities have been placed into DRAM array 1703. In the embodiment of FIG. 7*b*, these pools are T1 pool 1751, DS0 pool 1752, and VBR pool 1753. As previously described, these pools are typically assigned priorities 1, 2, and 3, respectively. Appropriate addressing techniques are used to indicate within a given one of these pools 1751 through 1753 which pointer should be used next to transfer cell information from Dram array 1703 to serial access memory 1704*b* for transfer to cell bus 403.

In the example shown in FIG. 7*b*, with the various pointer information stored in the pools as shown in FIG. 7*b*, cell data will be transferred from DRAM 1703 to output queue in the following sequence: PTR1, PTR3, PTR7, PTR2, PTR5, PTR7, and PTR4. Of course, if is likely that additional cell data will be received from the ATM switch for storage in DRAM array 1703 before this sequence of cell data transfer from Dram array 1703 is accomplished. In this event, additional pointers will be loaded into various ones of pools 1751 through 1753, and the above sequence of transfer of cell data from DRAM array 1703 will be altered due to the additional pointers stored in the pools.

When each cell of data is transferred from Dram array 1703 to SAM 1704*b*, that pointer is removed from the appropriate one of pools 1751 through 1753 and placed back into free pool 1750, indicating that that cell location within

DRAM array **1703** is once again available for storage of an incoming cell of data received from the ATM network.

In operation under the control of a microprocessor (not shown), when SAM **1704***b* is available following a transfer of its contents to the cell bus, the microprocessor causes a transfer of the currently indexed pointer from the highest priority nonempty queue formed by pools **1751** through **1753**.

Thus, in accordance with the teachings of this invention, the significant amount of data forming the data cells is read from the ATM serially into SAM **1704***a*, transferred in parallel fashion to DRAM array **1703**, and later transferred to SAM **1704***b* for serial transmission to cell bus **403**. During this time, there is very little manipulation of the cell data itself since it is simply stored in video RAM **1701**. However, in accordance with the teachings of this invention, a significant amount of manipulation is performed utilizing a standard microprocessor and series of pointer pools indicating the location of various data cells within video RAM **1701**. Thus, in accordance with the teachings of this invention, a relatively slow (as compared with high power/high cost SRAM) video RAM is used to store cell information, and the variety of manipulations to determine pointer information is achieved quickly since pointers are relatively short (typically 16 bits, as compared with a typical cell size of 424 bits).

FIG. **8** depicts one embodiment of HDLC controller **800** which is suitable for use in framing a plurality of channels. Shown in FIG. **8**, a T1 signal includes a plurality of separate channels (for example 24) which are multiplexed so that each channel provides eight bits of data at a time. As previously described with respect to FIG. **5**, HDLC framers **533** and **573** must provide the appropriate framing of data for a given channel of the T1 carrier. HDLC **800** serves to perform the HDLC framing function for a number of channels simultaneously, thereby minimizing circuit complexity and cost as compared with the prior art which would provide a dedicated HDLC framer for each one of the T1 channels. HDLC conversion is required in order to ensure the detection, accuracy and delineation of frames or packets of information and entails the following operation:

1) Flag insertion and deletion. In one embodiment, a flag is defined as a "0111 1110" binary bit pattern.

2) Zero stuffing and destuffing of the frame or packet data. This is the insertion of a binary bit "zero" into the frame or packet data stream after five "ones" have been sent. This ensures that a sequence resembling a "flag" is not contained in the frame or packet data stream.

3) Cyclic Redundancy Check (CRC) calculation. This is done to ensure the accuracy of the data bit within the frame or packet. When a frame or packet is transmitted, a CRC is generated incorporating the transmitted data pattern and is appended to the frame. At the receiving end, the reverse CRC is generated on the same data then compared to the CRC that was appended to the received frame or packet. If a correct match is found then the frame or packet is accepted as accurate. If a correct match is not found, the packet is discarded.

4) Detection and generation of an "abort" sequence. An abort sequence is defined as seven consecutive binary bit ones ("1111111"). Reception of an abort sequence forces the receive HDLC controller to immediately terminate and discard the frame currently being received. Generation of an abort sequence is only done when a non-recoverable error event occurs during transmission of a frame or packet that would severely compromise the accuracy of the data contained within.

Thus, the HDLC conversion must be performed on the entire set of bits in a frame. In accordance with the teachings of this invention, rather than providing a separate HDLC controller for each channel so that an entire frame of data can be accumulated for each channel prior to operation of its associated HDLC controller, the present invention utilizes a single TIME multiplexed HDLC controller **800**. HDLC controller **800** operates sequentially under each channel. As each of the eight bits of each channel is received the eight bits of data are stored in data buffer **803**. As HDLC **800** manipulates a given channel when eight bits of the channel data are received, HDLC controller **800** takes a state associated with that channel stored in state register **800** and transfers it to state pool **802**. As the next eight bits of data are received on the next sequential T1 channel, HDLC controller **800** receives the stored state associated with that channel from state pool **802** and stores it in state register **801**. HDLC controller **801** then utilizes that state and the newly received eight bits of that channel in order to further perform the HDLC conversion, arriving at a new intermediate state. That intermediate state is replaced in state pool **802**, the eight data bits transferred from data buffer **803** to the appropriate one of memories **804** through **804-24** correspond to the channel to which the eight bits of data belongs, and the interim state previously stored for the next adjacent channel is retrieved from state pool **802** and placed in state register **801**, allowing HDLC controller **800** to continue the HDLC conversion on the next eight bits received from the next sequential channel. Thus, the operation of HDLC controller **800**, in the T1 receive direction, may be described as follows, for an example applicable to a T1 system having 24 channels and N octets per frame:

1) initialize state (CH1)—state (CH24) in state pool **802** For i=1 to N For j=1 to 24
2) receive with set of 8 bits of channel j
3) retrieve intermediate HDLC state of channel j from pool **802**
4) perform HDLC flag detection/deletion, zero destuffing, abort detection and CRC checking
5) store intermediate HDLC state of channel j in pool **802**
6) store the resultant output data **803** in data pool **804**-j
7) next j
8) next i

The operation of HDLC controller **800**, in the T1 transmit direction, may be described as follows for the same example:

initialize state (CH1)—state (CH24) in state pool **802** For i=1 to N For j=1 to 24
2) receive with set of 8 bits of data pool **804**-J
3) retrieve intermediate HDLC state of channel j from pool **802**
4) perform HDLC flag insertion, zero stuffing, abort generation and CRC generation/insertion
5) store intermediate HDLC state of channel j in pool **802**
6) transmit the resultant output T1 data in channel j
7) next j
8) next i

FIG. **9** is a block diagram showing in more detail the transmit operation of HDLC controller **800** of FIG. **8**. In the transmit mode, the data to be applied to HDLC controller **800** is stored in buffer memory **804**. The data is arranged in buffer memory pages **804-1** through **804-24**, corresponding to the outgoing data channels and the state information stored in memory **802**. Address generator **902** generates the

channel address, in sequence. Channel configuration circuit **907** stores the channel data relationship descriptions. These descriptions determine when multiple channels are to be treated as a larger single channel, or if all channels should be treated separately. Main controller **901**, in conjunction with address generator **902**, uses the control signals from T1 Interface **908** and channel configuration **907** to produce the addresses to retrieve the corresponding buffer memory page from buffer memory **804** and the corresponding state from context memory **802**. The state is first loaded into circuits **903, 904, 905**, and **906** then the data from buffer memory **804** is clocked into new byte circuit **903**. This byte then is examined to determine if zero insertion, flag insertion and/or CRC generation is to be performed on this byte. Zero insertion circuit **904** will insert a zero after five consecutive logical ones have been detected in the combination of the new byte and previous byte. The previous byte's logical one content is part of the state data retrieved from context memory **802**. Flag insertion is performed by flag insertion circuitry **905**. Flag insertions will occur if there is no data in buffer memory **804** for the corresponding channel. CRC generator **906** performs the CRC on the non-flag data and sends this CRC when no data is detected in buffer memory **804**. The resultant data from circuits **903, 904, 905** and **906** is sent to T1 interface circuit **908** for transmission to the DS1 port in the corresponding channel.

Referring to FIG. **10**, in the receive mode, the data to be applied to HDLC controller **800**, received by T1 interface **908** prior to storage in buffer memory **804**. The data is arranged in buffer memory pages **804-1** through **804-24**, corresponding to-the outgoing data channels and the state information stored in memory **802**. Address generator **902** generates the channel address, in sequence. Channel configuration circuit **907** stores the channel data relationship descriptions. These descriptions determine when multiple channels are to be treated as a larger single channel, or if all channels should be treated separately. Main controller **901**, in conjunction with address generator **902**, uses the control signals from T1 Interface **908** and channel configuration **907** to produce the addresses to apply incoming data to the corresponding buffer memory page from buffer memory **804** and the corresponding state to context memory **802**. The state is first loaded into circuits **903, 904, 1009, 1005**, and **906** then the data from T1 interface **908** is clocked into new byte circuit **903**. This byte is examined by flag detection circuit **904**, and if it is determined to be a flag it will then be deleted (and not entered into Buffer memory **804**), otherwise flag detection circuit **904** will not take any action. If it is a flag and the previous byte was a data byte, then a CRC check will be performed by CRC checker **906** and the results will be stored in buffer memory **804**. If the new byte is not a flag, then it is then examined by Abort detection circuit **1009**. If it is an Abort sequence, then this indication is stored in buffer memory **804** and the data frame is considered terminated, and no CRC is stored. If it is not an abort sequence, then the new byte is examined for five consecutive logical ones in the combination of the new byte and the previous byte (whose state was retrieved from the context memory **802**). If so, then the following zero will be deleted before it is stored in buffer memory **804**. The data in buffer memory **804** is then segmented into ATM cells for transmission unto the cell bus.

The above described embodiments are referenced to T1 and T3 carriers, although it is to be appreciated that the teachings of this invention are suitable for use with any appropriate or desirable bandwidths and data lengths. For example, while T1 is a North American standard capable of carrying 24 simultaneous voice/data channels, much of the world uses the E1 standard, capable of carrying 32 simultaneous voice/data channels at a bandwidth of 2.048 megabits/second. In one embodiment of this invention, the system is designed for the E1 standard, capable of handling 32 simultaneous voice/data channels. When this embodiment is used in a T1 environment, such as North America, eight channels are simply not used or saved as spares, thereby allowing a single product capable of handling 32 simultaneous voice data channels under the E1 standard to be used both under the E1 standard and the T1 standard.

All publications and patent applications mentioned in this specification are herein incorporated by reference to the same extent as if each individual publication or patent application was specifically and individually indicated to be incorporated by reference.

The invention now being fully described, it will be apparent to one of ordinary skill in the art that many changes and modifications can be made thereto without departing from the spirit or scope of the appended claims.

What is claimed is:

1. An ATM network interface comprising:

an input port for receiving data for placement on said ATM network;

an output port coupled to said ATM network;

a memory array for storing said data received on said input port until said data is placed on said ATM network via said output port;

plurality of pointer pools, each comprising a plurality of locations for storing pointers serving to address a portion of said data stored in said memory array;

a control circuit for storing within said pointer pools addresses corresponding to data stored in said memory array based on a priority for which said data stored in said memory array is to be output to said ATM network via said output port; and

a network interface output queue coupled between said memory array and said output port for temporarily storing data read out from said memory array as a function of said priorities, prior to said data being placed on said ATM network.

2. An ATM network interface comprising:

an input port for receiving data for placement on said ATM network;

an output port coupled to said ATM network;

a memory array for storing said data received on said input port until said data is placed on said ATM network via said output port;

a plurality of pointer pools, each comprising a plurality of locations for storing pointers serving to address a portion of said data stored in said memory array, said plurality of pointer pools each having an associated priority, and entries are stored within a selected one of said pointer pools on the basis of priority of data; and

a control circuit for storing within said pointer pools addresses corresponding to data stored in said memory array based on a priority for which said data stored in said memory array is to be output to said ATM network via said output port.

3. An ATM network interface as in claim **2** wherein said priorities associated with said pointer pools are established by data types.

4. An ATM network interface comprising:

an input port for receiving data for placement on said ATM network;

an output port coupled to said ATM network;

a memory array for storing said data received on said input port until said data is placed on said ATM network via said output port, said memory array comprising:

a serial input port coupled to said input port of said ATM network interface;

a serial output port coupled to said output port of said ATM network interface;

an input serial access memory coupled to said serial input port;

an output serial access memory coupled to said serial output port; and

a word oriented memory array which receives data for storage from said input serial access memory as a set of data bits in parallel and which provides data to said output serial access memory as a set of data bits in parallel; and

a plurality of pointer pools, each comprising a plurality of locations for storing pointers serving to address a portion of said data stored in said memory array; and

a control circuit for storing within said pointer pools addresses corresponding to data stored in said memory array based on a priority for which said data stored in said memory array is to be output to said ATM network via said output port.

5. An ATM network interface as in claim **4** wherein said memory array comprises a VRAM.

6. An ATM network interface comprising:

an input port for receiving data for placement on said ATM network;

an output port coupled to said ATM network;

a memory array for storing said data received on said input port until said data is placed on said ATM network via said output port;

a plurality of pointer pools, each comprising a plurality of locations for storing pointers serving to address a portion of said data stored in said memory array;

a control circuit for storing within said pointer pools addresses corresponding to data stored in said memory array based on a priority for which said data stored in said memory array is to be output to said ATM network via said output port; and

a free pool which stores the available addresses of said memory array where newly received data can be stored.

7. An ATM network interface comprising:

an input port for receiving data for placement on said ATM network;

an output port coupled to said ATM network;

a memory array for storing said data received on said input port until said data is placed on said ATM network via said output port;

a plurality of pointer pools, each comprising a plurality of locations for storing pointers serving to address a portion of said data stored in said memory array;

a control circuit for storing within said pointer pools addresses corresponding to data stored in said memory array based on a priority for which said data stored in said memory array is to be output to said ATM network via said output port; and

a traffic shaping ring comprising a memory for storing a plurality of said pointers output from said pointer pools based on said priorities, and circuitry for sequentially removing said pointers from said traffic shaping ring and causing said data stored within said memory array associated therewith to be placed on said ATM network.

8. An ATM network interface as in claim **7** wherein said priority is established, at least in part, based on the receive capacity of a destination.

9. An ATM network interface comprising:

a plurality of output ports coupled to one or more users;

an input port for receiving data from said ATM network, said input port having a bandwidth less than the sum of the bandwidths of said plurality of output ports;

a memory array for storing said data received on said input port until said data is sent to said users via said output port;

a plurality of pointer pools, each comprising a plurality of locations for storing pointers serving to address a portion of said data stored in said memory array; and

a control circuit for storing within said pointer pools addresses corresponding to data stored in said memory array based on a priority for which said data stored in said memory array is to be output to said users via said output port.

10. An ATM network interface comprising:

an input port for receiving data from said ATM network;

an output port coupled to one or more users;

a memory array for storing said data received on said input port until said data is sent to said users via said output port;

a plurality of pointer pools, each comprising a plurality of locations for storing pointers serving to address a portion of said data stored in said memory array, said plurality of pointer pools each having an associated priority, and entries are stored within a selected one of said pointer pools on the basis of priority of data; and

a control circuit for storing within said pointer pools addresses corresponding to data stored in said memory array based on a priority for which said data stored in said memory array is to be output to said users via said output port.

11. An ATM network interface as in claim **10** wherein said priorities associated with said pointer pools are established by data types.

12. An ATM network interface comprising:

an input port for receiving data from said ATM network;

an output port coupled to one or more users;

a memory array for storing said data received on said input port until said data is sent to said users via said output port, said memory array comprising:

a serial input port coupled to said input port of said ATM network interface;

a serial output port coupled to said output port of said ATM network interface;

an input serial access memory coupled to said serial input port;

an output serial access memory coupled to said serial output port; and

a word oriented memory array which receives data for storage from said input serial access memory as a set of data bits in parallel and which provides data to said output serial access memory as a set of data bits in parallel; and

a plurality of pointer pools, each comprising a plurality of locations for storing pointers serving to address a portion of said data stored in said memory array; and

a control circuit for storing within said pointer pools addresses corresponding to data stored in said memory

array based on a priority for which said data stored in said memory array is to be output to said users via said output port.

13. An ATM network interface as in claim 12 wherein said memory array comprises a VRAM.

14. An ATM network interface comprising:

an input port for receiving data from said ATM network;

an output port coupled to one or more users;

a memory array for storing said data received on said input port until said data is sent to said users via said output port;

a plurality of pointer pools, each comprising a plurality of locations for storing pointers serving to address a portion of said data stored in said memory array;

a control circuit for storing within said pointer pools addresses corresponding to data stored in said memory array based on a priority for which said data stored in said memory array is to be output to said users via said output port; and

a free pool which stores the available addresses of said memory array where newly received data can be stored.

15. An ATM network interface comprising:

an input port for receiving data from said ATM network;

an output port coupled to one or more users;

a memory array for storing said data received on said input port until said data is sent to said users via said output port;

a plurality of pointer pools, each comprising a plurality of locations for storing pointers serving to address a portion of said data stored in said memory array;

a control circuit for storing within said pointer pools addresses corresponding to data stored in said memory array based on a priority for which said data stored in said memory array is to be output to said users via said output port; and

a traffic shaping ring comprising a memory for storing a plurality of said pointers output from said pointer pools based on said priorities, and circuitry for sequentially removing said pointers from said traffic shaping ring and causing said data stored within said memory array associated therewith to be placed on said output port.

16. An ATM network interface as in claim 15 wherein said priority is established, at least in part, based on the receive capacity of a destination.

17. A method for operating an ATM network interface comprising the steps of:

receiving input data;

storing said data in a memory;

maintaining a plurality of pointer pools, each storing a set of pointers serving as addresses associated with said data stored in said memory;

moving said pointers from said pointer pools to a traffic shaping ring; and

outputting data from said memory based on the order of pointers on said traffic shaping ring, wherein pointers are stored within said pointer pools based on priority of data.

18. A method for operating an ATM network interface comprising the steps of:

receiving input data;

storing said data in a memory;

maintaining a plurality of pointer pools, each storing a set of pointers serving as addresses associated with said data stored in said memory;

moving said pointers from said pointer pools to a traffic shaping ring; and

outputting data from said memory based on the order of pointers on said traffic shaping ring, wherein said pointers are placed on said traffic shaping ring based on priority of data.

19. A method as in claim 18 wherein said priority of .data is established, at least in part, based on the receive capacity of a destination.

20. An HDLC controller comprising:

an input port for receiving data;

an output port;

a first memory comprising a plurality of memory sections, each associated with a channel of data;

a second memory comprising a plurality of memory sections, each for storing state information associated with a given one of said channels of data;

control circuitry for retrieving from said second memory state information associated with a channel of data being received;

HDLC manipulation circuitry for performing an HDLC operation on said channel of data being received, in conjunction with said retrieved state information corresponding to previous data received for the same channel of data;

control circuitry for updating said state information associated with said channel of data and storing the updated state information in said second memory; and

control circuitry for transferring the result of said HDLC operation to the appropriate one of said memory locations within said first memory.

21. A multi-channel network interface controller comprising.:

an input port for receiving data from a plurality of data channels;

an output port;

a first memory comprising a plurality of memory sections, each associated with one of said data channels;

a second memory comprising a plurality of memory sections, each for storing state information associated with a given one of said data channels;

control circuitry for retrieving from said second memory state information associated with a data channel being received;

manipulation circuitry for performing an operation on said channel of data being received, in conjunction with said retrieved state information corresponding to previous data received for the same data channel;

control circuitry for updating said state information associated with said data channel and storing the updated state information in said second memory; and

control circuitry for transferring the result of said operation to the appropriate one of said memory locations within said first memory.

22. A device as in claim 21 wherein said manipulation circuitry further comprises a set of instructions defining said operation based, at least in part, by the format of data received from one or more of said data channels.

23. An ATM network interface comprising:

an plurality of input ports for receiving data for placement on said ATM network;

an output port coupled to said ATM network, the bandwidth of said output port being less than the sum of the bandwidths of said plurality of input ports;

a memory array for storing said data received on said input port until said data is placed on said ATM network via said output port;

a plurality of pointer pools, each comprising a plurality of locations for storing pointers serving to address a portion of said. data stored in said memory array; and

a control circuit for storing within said pointer pools addresses corresponding to data stored in said memory array based on a priority for which said data stored in said memory array is to be output to said ATM network via said output port.

* * * * *

US005579324A

United States Patent [19]

Buhrgard

[11] Patent Number: 5,579,324

[45] Date of Patent: Nov. 26, 1996

[54] **SYNCHRONIZING CIRCUIT ARRANGEMENT**

[75] Inventor: **Karl S. M. Buhrgard**, Stockholm, Sweden

[73] Assignee: **Telefonaktiebolaget LM Ericsson**, Stockholm, Sweden

[21] Appl. No.: **320,661**

[22] Filed: **Oct. 11, 1994**

[30] **Foreign Application Priority Data**

Oct. 12, 1993 [SE] Sweden 93033413

[51] **Int. Cl.**[6] **H04J 3/06**

[52] **U.S. Cl.** **370/105.1**; 370/112; 371/42

[58] **Field of Search** 370/100.1, 105.1, 370/105.3, 105.4, 106, 108, 94.1, 112, 13; 375/365, 356, 368, 372; 371/37.1, 37.7, 47.1, 42

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,788,681	11/1988	Thomas et al.	370/105.1
4,796,282	1/1989	Yoshida	375/368
4,873,663	10/1989	Baranyai et al.	370/100.1
4,894,826	1/1990	Aggers et al.	370/13
4,922,438	5/1990	Ballweg	370/105.3
5,014,272	5/1991	Yoshida	370/105.1
5,107,495	4/1992	Kamoi et al.	370/100.1
5,130,984	7/1992	Cisneros	370/94.1
5,131,012	7/1992	Dravida	371/42
5,345,451	9/1994	Uriu et al.	371/42
5,367,544	11/1994	Bruekheimer	371/42

FOREIGN PATENT DOCUMENTS

WO93/19986 10/1993 WIPO .

Primary Examiner—Douglas W. Olms
Assistant Examiner—Chau T. Nguyen
Attorney, Agent, or Firm—Burns, Doane, Swecker & Mathis, L.L.P.

[57] **ABSTRACT**

A synchronizing circuit arrangement included in a multiplexing/demultiplexing unit receives a bit stream coordinated to a data packet. The bit positions and values within a predetermined part of a consecutive bit sequence of each transmitted data packet are constantly selected so that a predetermined check calculation will give a predetermined value (for instance, "0"). A consecutive bit sequence corresponding to the predetermined part of a consecutive bit sequence and belonging to respective received data packets is evaluated in order to establish the extent to which the check calculation gives the predetermined value. When agreement is found, it is assumed that the boundary between two closely adjacent data packets is established via the bit sequence of the predetermined part of a consecutive bit sequence. Each incoming bit stream is synchronized through the medium of a control block or control logic by inserting a time delay corresponding to synchronism into a series-parallel converter for respective bit streams. The synchronized, parallel-format bit streams can be delivered via the control block or control logic to a memory which delivers the bit stream to the outgoing connection via buffer circuits and a parallel-series converter.

19 Claims, 2 Drawing Sheets

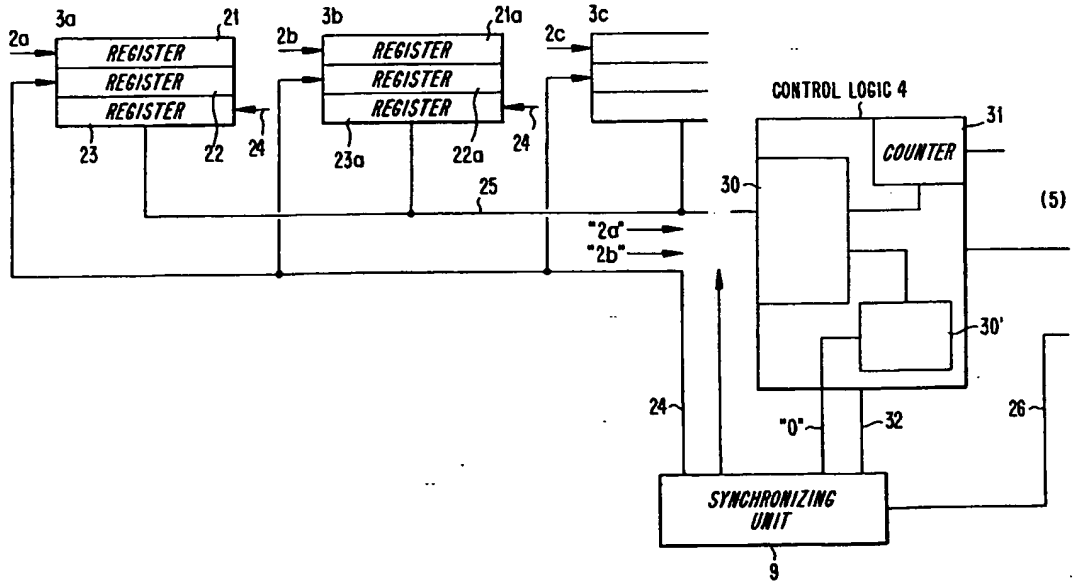


Fig. 1

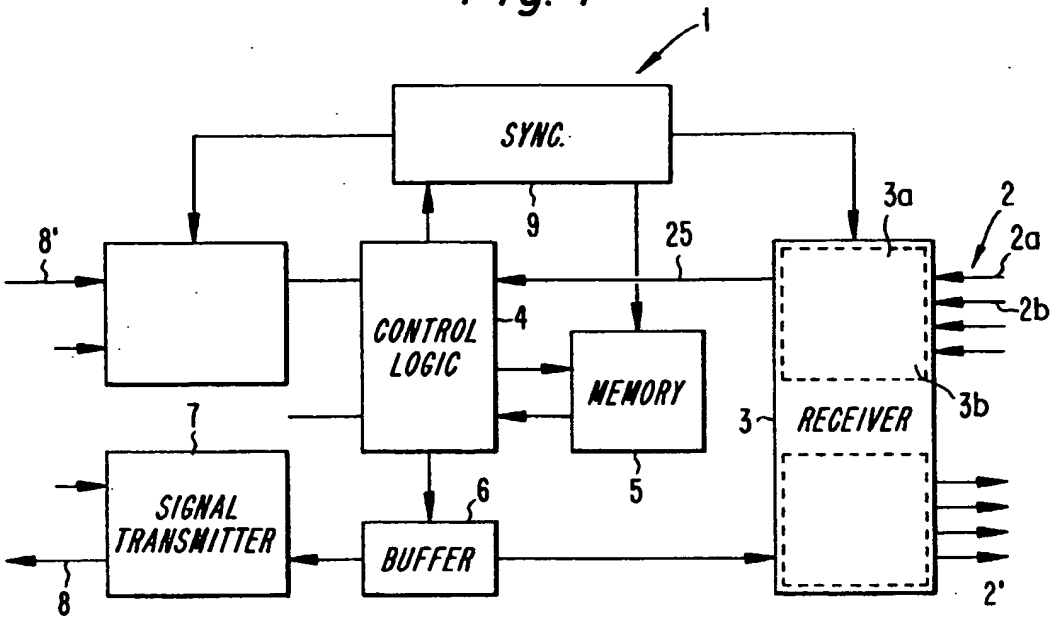
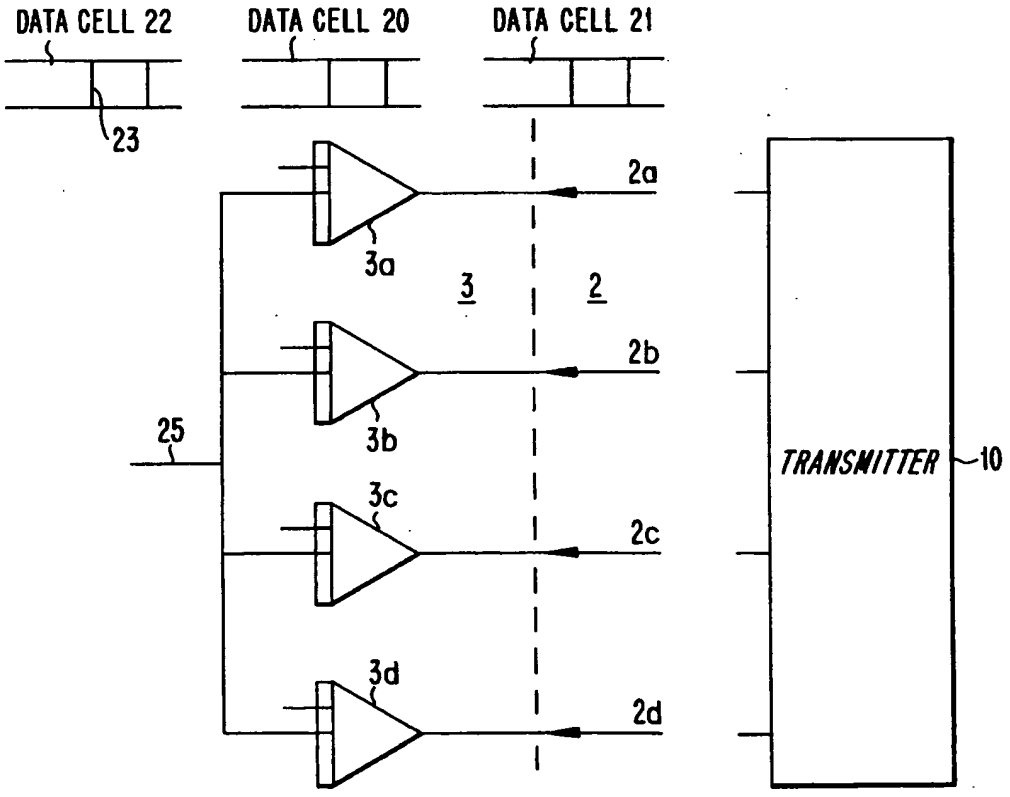

1
SYNC.
9
25
3a
2
2a
2b
8'
CONTROL LOGIC
4
MEMORY
3
RECEIVER
3b
7
SIGNAL TRANSMITTER
6
BUFFER
5
8
2'

Fig. 2


DATA CELL 22
DATA CELL 20
DATA CELL 21
23
2a
3a
3
2
2b
3b
25
3c
2c
3d
2d
TRANSMITTER
10

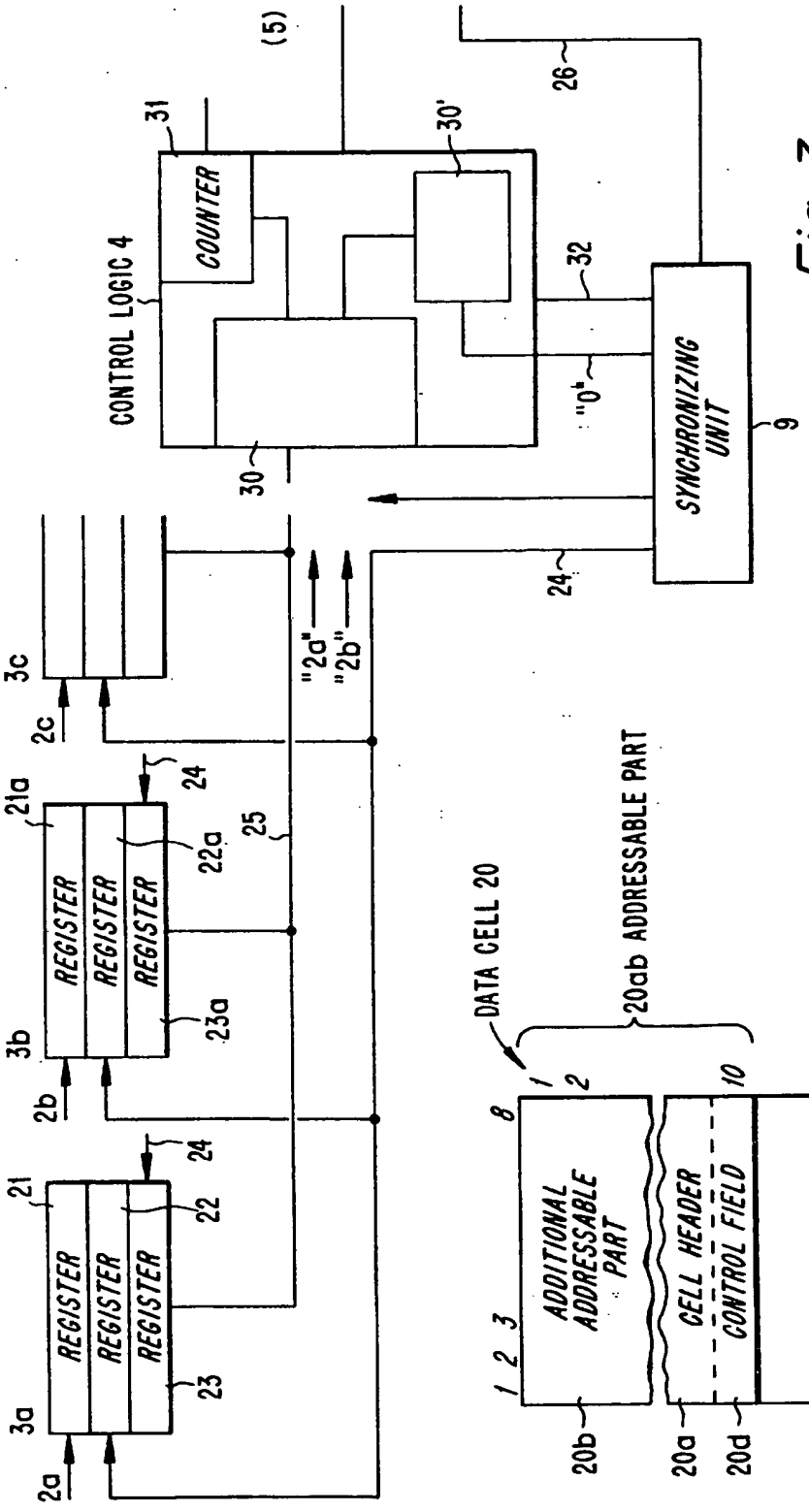

(5)
26
31
30'
COUNTER
CONTROL LOGIC 4
32
"0"
SYNCHRONIZING UNIT
9
30
24
"2a"
"2b"
3c
2c
24
21a
25
22a
REGISTER
REGISTER
REGISTER
3b
23a
2b
24
21
22
REGISTER
REGISTER
REGISTER
3a
23
2a

Fig. 3

DATA CELL 20
20ab ADDRESSABLE PART
1
2
8
10
60
ADDITIONAL ADDRESSABLE PART
CELL HEADER
CONTROL FIELD
INFORMATION CARRYING PART
1 2 3
20b
20a
20d
20c

Fig. 4

SYNCHRONIZING CIRCUIT ARRANGEMENT

TECHNICAL FIELD

The present invention relates to a synchronizing circuit arrangement and then more particularly, but not exclusively, to a synchronizing circuit arrangement adapted for use in a multiplexing/demultiplexing unit.

Such units are used to increase or decrease the transmission rate of pulsated signal streams, so-called bit streams, occurring on connections.

The invention finds particular use when the pulsated signals within the bit stream are coordinated to form data packets or data cells having an address indicating section and an information-carrying section, preferably structured in the manner described in the ATM system.

The inventive synchronizing circuit arrangement is based on the ability to establish in one or more sequentially occurring and orientated bit streams grouped in closely following and clearly determined data packets a relevant boundary between two, mutually adjacent and closely sequential data packets with the aid of a receiving circuit, and therewith create provisions for synchronizing received data packets with a synchronizing signal in said receiver.

The invention is also based on the possibility of establishing an "interface" or a "boundary" between two mutually sequential data packets, where the last bit position of a preceding data packet is immediately followed by the first bit position of an immediately following data packet.

DESCRIPTION OF THE BACKGROUND ART

Synchronizing circuit arrangements of the aforedefined kind are known to the art and are also standardized. For instance, it is known to provide in a multiplexing/demultiplexing unit a synchronizing circuit arrangement for synchronizing bit streams that are coordinated to form a data packet and to use the principle of dividing each data packet into an address-carrying section and an information-carrying section, and to divide the whole of the data packet into a given number of parts, one or more bytes or words. When practicing known techniques, a boundary can be established between two closely following data packets in a sequentially oriented bit stream divided into mutually sequential and clearly defined data packets, by constantly giving the bit positions a positional value within a predetermined defined part of a consecutive bit sequence of each transmitted data packet so that they will have a given value (for instance "0") predetermined by a predetermined check or control calculation.

A bit sequence belonging to a respective received data packet and corresponding to the aforesaid determined part of a consecutive bit sequence is evaluated in order to establish the extent to which said check calculation will give the predetermined value.

When agreement is found, the boundary between two mutually sequential data packets is established via the bit sequence of the selected part.

In the case of a multiplexing function, the bit stream coordinated within the data packet will occur on a number of incoming connections at a bit rate higher than 100 Mb/s and then at a higher rate on an outgoing connection, whereas the reverse applies in the case of a demultiplexing function, without changing the information content of the data packet.

With regard to the embodiment that describes the present invention, it can be mentioned that it is known to supplement a standardized ATM data cell or ATM data packet with an additional information-carrying bit position section which is intended to provide switch-internal address information and which is added to the standardized ATM data cell at the input to the switch unit and is removed at the output thereof.

An example of the earlier standpoint of technique in this regard is illustrated and described in U.S. Pat. No. 5,130,984.

SUMMARY OF THE INVENTION

TECHNICAL PROBLEMS

When considering the known prior art as described above, it will be seen that a technical problem resides in providing a synchronizing circuit arrangement which will enable a receiving unit to determine or establish a boundary between mutually adjacent and closely following data packets and which will enable each incoming bit stream to be synchronized with the aid of simple functional means, such as an integrated circuit, through the medium of a control block or control logic, by applying to a series-parallel converter for respective bit streams a time delay which corresponds to the synchronism required, wherein the resultant parallel-formatized synchronized bit streams can be supplied through said control block or control logic to a memory which delivers the bit stream on the outgoing connection through the medium of buffer circuits and a parallel-series converter.

It will also be seen that another technical problem is one of realizing the advantages that are associated with choosing the address-carrying standardized section in an ATM data cell or the like, or a combination of this section and an added section as a reference section or part, so as to provide switch-internal address information.

A further technical problem is one of realizing the advantages that are associated with selecting from each data-packet bit sequence a predetermined part and then dividing this part into a predetermined number of sub-sections.

It will also be seen that a technical problem is one of realizing the necessity of utilizing the fact that the value of the bit positions within said sections in transmission must constantly be so selected that they will always provide a predetermined value that is recognizable by the receiver in a predetermined check calculation or chosen parity check.

It will also be seen that a technical problem is one of realizing the significance in evaluating in the receiving unit a consecutive bit sequence belonging to respective data packets and equal to or exceeding said part simultaneously, so as to establish the extent to which each of the subsections accommodated therein gives the predetermined value in the check calculation.

Another technical problem is one of realizing the significance that when agreement occurs between a calculated result from a check calculation or parity check inserted in the receiving unit for the sub-sections of respective data packets and a given value, that the bit sequence concerned within respective subsections is able to initiate synchronism, therewith enabling the boundary between two mutually adjacent and closely following data packets to be established.

It will also be seen that a technical problem resides in realizing those advantages that are afforded when the whole of the determined part is comprised exactly of an addressable part of respective data packets.

Another technical problem is one of providing with the aid of simple means conditions which will enable the section to be divided into individual sub-sections in accordance with the number of bit positions, and that the number of sub-sections is chosen for an ATM data cell with or without an additional switch-internal addressing information to at least four.

It will also be seen that a technical problem resides in realizing the degree of reliability that is achieved and therewith the advantages that are afforded when the boundary is not established until agreement is found between calculated and anticipated results from the check calculation or parity check for respective sub-sections relating to a predetermined number of mutually sequential data packets.

Another technical problem is one of realizing that when there is no agreement, it is necessary to carry out a search which involves moving a given part of a consecutive bit sequence through one bit position forwards or backwards and then making a check calculation on the new part with the sub-section in the same manner throughout the entire data packet and not to establish the boundary until agreement is found between the obtained result and the anticipated result from the check calculation or the parity check for respective sub-sections, and to again move the determined part through one bit position in the same direction when agreement is still not found.

SOLUTION

The present invention solves one or more of the aforesaid technical problems with the aid of a synchronizing circuit arrangement of the kind defined in the introduction and in the preamble of the following Claim 1.

Accordingly, in accordance with the present invention, each incoming bit stream is synchronized with the aid of an integrated circuit and a control block or control logic formed thereby by inserting in a series-parallel converter for respective bit streams a time delay which corresponds to synchronism, wherein synchronized bit streams occurring in a parallel format are delivered to a memory via the control or control logic, and wherein the bit streams are delivered on said outgoing connection at a changed bit rate, via buffer circuits and a parallel-series conversion. According to proposed embodiments lying within the scope of the inventive concept, the aforesaid given part of a consecutive bit sequence is comprised of an addressable part of respective data packets.

It is also suggested that said part is divided into a predetermined number of sub-sections, for instance four sub-sections.

According to one preferred embodiment of the invention, the boundary is not established until agreement has repeatedly been established for a predetermined number of mutually sequential data packets.

It is also proposed that when agreement is not found, the given part of a consecutive bit sequence is moved within said consecutive bit sequence by one bit position, either forwards or backwards, and that a new check calculation is made on the new part within the control unit in the same way, so that the new boundary can be established when agreement is found, whereas if agreement is not found the given part is again moved one bit position in the same direction.

ADVANTAGES

Those advantages primarily characteristic of an inventive synchronizing circuit arrangement reside in the possibility of establishing the boundary between two incoming and immediately following data packets among a continuous stream of data packets, and in the ability of creating conditions for each incoming bit stream on each connection that will enable a time delay corresponding to synchronism to be inserted so that all bit streams that are able to occur as a grouped logic link incoming to a control block or control logic will obtain synchronous and coordinated storage in a memory and be delivered therefrom serially and in sequence to an outgoing connection.

The main characteristic features of the inventive synchronizing circuit arrangement are set forth in the characterizing clause of the following claim 1.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will now be described in more detail with reference to an exemplifying embodiment of an arrangement which functions in accordance with the principles of the invention, and also with reference to the accompanying drawings, in which

FIG. 1 illustrates an integrated circuit for a multiplexing/demultiplexing unit having four incoming connections and one outgoing connection, or vice versa;

FIG. 2 illustrates schematically a transmitter and a series-parallel converter coordinated in a receiver to four incoming connections;

FIG. 3 is a principle diagram illustrating a function block arrangement for series-parallel conversion, and also shows coaction with a control block or control logic; and

FIG. 4 illustrates the orientation of the bit positions in a standardized ATM data cell with an additional section for switch-internal addressing.

DESCRIPTION OF EMBODIMENTS AT PRESENT PREFERRED

FIG. 1 is a block schematic which illustrates a multiplexing/demultiplexing unit 1 in the form of an integrated circuit.

The unit 1 has four incoming connections 2 which are connected to a signal-receiving circuit 3 which itself is connected (25) to a control block or control logic 4 coacting with a memory and a buffer circuit 6 which through the medium of a signal-transmitting circuit 7 functions to transmit a bit stream in series form on a connection 8 adapted to a rate which exceeds the rate at which respective bit streams occur on each of the four incoming connections 2.

Also shown in FIG. 1 is a synchronizing arrangement 9 which will be described below in more detail, together with the control logic 4.

The unit 1 is also adapted to perform a demultiplexing function and is intended to receive on connection 8' a bit stream series and to break up the bit streams into four parallel bit streams over a respective outgoing connection 2'.

For the sake of simplicity, the following description will be made primarily with reference to the multiplexing function.

FIG. 2 illustrates a transmitter 10 which is able to transmit a sequentially orientated bit stream on each of four connections 2*a*, 2*b*, 2*c* and 2*d*. The bit streams are mutually shifted slightly in time and are structured as data packets which follow one another in close succession and which together form a grouped logic link. The bit positions of an ATM-related data cell are shown in FIG. 4.

As shown in FIG. 2, for each connection a data cell **20** is preceded by a data cell **21** and is followed by a data cell **22**, where the last bit position of a data cell occurs immediately adjacent the first bit position of an immediately following data cell.

Each such data packet or data cell, such as the data packet **20** in FIG. 4, is comprised of 60 octets, wherein a standardized addressable part or a cell header **20***a* is comprised of 5 octets, an additional addressable part **20***b* is also comprised of 5 octets and relates to an internally usable address part which is added upon entry of the data cell into a switch and is removed when the data cells leave the switch.

The data packet also includes an information-carrying part or payload part **20***c*.

Such a data cell will thus have a total of 480 bit positions divided into 60 octets.

The invention is based on the necessity of each data packet used including a predetermined number of bit positions. According to the invention, it shall be possible to divide or coordinate some of these bit positions in a predetermined number of units or parts.

This is illustrated in the exemplifying embodiment insomuch that the data cell **20** includes a first section **20***ab* (including two sub-sections **20***a*, **20***b*) and a second section **20***c*.

It will also be seen that the section **20***ab* includes a number of bit positions **20***d* (one byte sorted in the field **10**), which are intended for bit positions representing a control field.

The invention is based on the use primarily of the section **20***ab* and the control field **20***d*.

The transmitter **10** includes known means which give the field **20***d* a bit configuration representative of the value of a check calculation carried out in the transmitter **10** in accordance with a chosen algorithm or via a parity check of the bit positions in the remainder of the section **20***ab*.

The algorithm chosen or the parity check carried out on the section **20***ab* shall be given a value which can be recognized by the receiver, this value being assumed to be always "0" for the sake of simplicity.

This section (**20***ab*) will be transmitted by the transmitter **10** together with remaining bit positions (**20***c*) of the data cell to the receiving unit **3** via the connections **2** on respective lines **2***a*–**2***d*.

It will be noted that even though all data packets should be transmitted simultaneously and in synchronism from the transmitter **10** over the four lines **2***a*, **2***b*, **2***c* and **2***d* to the receiver **3**, it can be assumed that these data packets will not all arrive at the receiver **3** in synchronism and at one and the same time. Even though the data packets are consciously transmitted while displaced in time in accordance with the principles illustrated and described in publication PCT/SE93/00277, it would still be necessary to synchronize to a selected time shift.

It is thus necessary to synchronize all received signals in the unit **1**.

The principles and functions of the invention will be described initially with reference to the case in which the bit positions on the connection **2***a* arrive at the receiving circuit **3***a* in synchronism with a synchronizing signal belonging to or generated by the receiver **3**.

As illustrated in FIG. 2, the serially occurring data packets **20** on the connection **2***a* are delivered to a series-parallel converter **3***a*, wherein the bit positions of the data packets are divided into parallel-transmittable 20-bit words on a line **25**.

As will be seen from FIG. 3, the bit stream on line **2***a* is delivered to a 20-bit register **21** and moved down to an adjacent register **22**.

The bit positions in the register **22** are moved to a register **23** which transfers the bit positions to the control unit **4** in response to an activating signal delivered on the line **24**.

The control unit **4** now calculates in a calculating circuit **30** the check sum for four mutually sequential 20-bit sequences and notes that the check sum is "0" wherein the control unit **4** indicates to the synchronizing unit **9** that the check sum was "0" wherewith the synchronizing unit **9** generates, via the line **26**, a signal for the beginning of the data packet and each 20-bit sequence can be stored in the memory **5**.

By way of a safety control feature, the control unit **4** waits, via a circuit **30'**, until the calculated bit positions give the value "0" over a number of data packets, for instance four data packets, before accepted synchronization is activated, there being required to this end a counter **31** which enables the total number of bit positions of the data packet to be observed.

Should this calculation not give the result "0", which is assumed to be the case for the line **2***b*, the control unit **4** sends a command to the synchronizing unit **9** on the line **32**, causing the register **22***a* to move one step or one bit position forwards, via the line **24**, whereafter a new calculation is made on four sequential 20-bit sequences belonging to the data packet. Alternatively register **22A** could be made to move one step or one bit position backward.

If the calculation results in the check sum "0", then synchronism exists, otherwise the register must again be stepped forwards and all the bit positions of the data packet calculated until synchronism is obtained.

In order for it to be possible to synchronize in this way, it is necessary for all bit positions of each data packet and the values assigned to said bit positions to fulfil at least certain basic criteria when transmitted.

These criteria can be summed up as follows:

a) Each data packet must have a predetermined number of bit positions and a predetermined rate, which is checked in the units **30** and **31**.

b) Each data packet will preferably be capable of being divided into a given number of units or parts in a precise manner, for instance two parts, such as the addressable part (**20***ab*) and the information-carrying part (20c).

c) One of these parts, for instance the addressable part (**20***ab*), shall be divisible uniformly into a number of equal sub-sections (for instance four sub-sections of 20-bit words).

d) When transmitting, it is necessary to have assigned to the bit positions within each such subsection (**20***a*, **20***b*) for respective data packets a bit configuration that corresponds to the desired transmission of information, and that a bit field (**20***d*) has also been supplemented with a configuration such that when all bit positions and their values have been checked, for instance by means of a calculating process **30** with the aid of a selected algorithm or with the aid of a parity check, the check will give one and the same value for each data packet.

e) Each alternate subsection (20c) will preferably not have a bit configuration which with the same number of bit positions as in the section (**20***ab*) and in response to a chosen calculating process or check process gives the same value.

The probability that such a selected sub-section within or between the given sub-sections **20***a*, **20***b* and **20***c* will give an anticipated value for each of a number of mutually sequential data packets shall be small.

The synchronizing logic **9** and/or the control logic **4** include a bit counter **31** so that the total number of bit positions of a data packet will be known and therewith enable the beginning and the end of a data packet to be established.

The same functional flow takes place in principle in the case of a demultiplexing function.

Parallel-formatted data packets originating from the lines **2***a*–**2***d* can now be delivered to the control logic **4** as a number of 20-bit words via a selected time delay. These 20-bit words are stored in the memory **5** which, in turn, delivers 20-bit words to a buffer circuit which transmits the data packets on a line or a connection **8**, via a parallel-series converter **7**.

It follows from this that in the case of a multiplexing function or a demultiplexing function in accordance with the present invention, a common synchronizing logic **9** can be used together with a common memory **5**, common buffer circuits **6**, etc.

A circuit arrangement of the kind described can be used advantageously with a unit described and illustrated in U.S. patent application Ser. No. 08/320,660 filed at the same time as the present application and entitled "A Signal Receiving and Signal

Transmitting Unit" or with a unit described and illustrated in U.S. patent application Ser. No. 08/321,180 filed at the same time as the present application and entitled "A Signal Processing Unit", or with a unit described and illustrated in U.S. patent application Ser. No. 08/320,659 filed at the same time as the present patent application and entitled "Multiplexing/Demultiplexing Unit".

Reference is made to these patent applications for a deeper understanding of the application of the present invention, and the contents of these patent applications shall be considered as forming part of the present application.

It will be understood that the invention is not restricted to the aforedescribed and illustrated exemplifying embodiment thereof and that modifications can be made within the scope of the inventive concept as defined in the following claims.

I claim:

1. A synchronizing circuit arrangement, comprising:

a multiplexing/demultiplexing unit for dividing a sequentially orientated bit stream into defined mutually sequential data packets thereby establishing a boundary between two closely adjacent data packets by constantly selecting the bit positions and values within a predetermined part of a consecutive bit sequence in each transmitted data packet so that a predetermined check calculation of the predetermined part will give a predetermined value; the multiplexing/demultiplexing unit including:

a control logic for synchronizing each incoming bit stream by inserting into a series-parallel converter for respective bit streams a time delay corresponding to synchronism;

a memory for receiving from the control logic in a parallel-format synchronized bit stream; and

an outgoing connection for receiving the parallel-format synchronized bit stream through buffer circuits and a parallel-series converter;

wherein a bit sequence belonging to received data packets and consecutive to the predetermined part of a consecutive bit sequence is evaluated to establish the extent to which the check calculation gives the predetermined value; and in the event of the check calculation and predetermined value agree, the multiplexing/demultiplexing unit establishes the boundary between two closely adjacent data packets through the bit sequence of the selected part; and in the case of a multiplexing function, the multiplexing/demultiplexing unit coordinates the bit stream into a data packet on a number of incoming connections and one outgoing connection establishing a grouped logic link, and in the case of a demultiplexing function the multiplexing/demultiplexing unit coordinates bit streams into data packets on one incoming connection and a number of outgoing connections establishing a grouped logic link.

2. An arrangement according to claim **1**, characterized in that said predetermined part of a consecutive bit sequence is comprised of an addressable part of respective data packets.

3. An arrangement according to claim **1**, characterized in that said predetermined part of a consecutive bit sequence is divided into a given number of sub-sections.

4. An arrangement according to claim **1**, characterized in that the boundary is not established until agreement is found with regard to a predetermined number of mutually sequential data packets.

5. An arrangement according to claim **1**, characterized in that when no agreement is found with any of the incoming connections (**2***a*–**2***d*), the predetermined part of a consecutive bit sequence is moved one bit position forwards or backwards, whereafter a check calculation is carried out on said part in the same way as earlier, so as to establish the boundary when agreement is found and so as to move the predetermined part through a further bit position in the same direction when no agreement is found.

6. An arrangement according to claim **1**, characterized in that said, predetermined part of a consecutive bit sequence is divided into at least four sub-sections.

7. An arrangement according to claim **2**, characterized in that said predetermined part of a consecutive bit sequence is divided into a given number of sub-sections.

8. An arrangement according to claim **7**, characterized in that said predetermined part of a consecutive bit sequence is divided into at least four sub-sections.

9. An arrangement according to claim **2**, characterized in that the boundary is not established until agreement is found with regard to a predetermined number of mutually sequential data packets.

10. An arrangement according to claim **3**, characterized in that the boundary is not established until agreement is found with regard to a predetermined number of mutually sequential data packets.

11. An arrangement according to claim **6**, characterized in that the boundary is not established until agreement is found with regard to a predetermined number of mutually sequential data packets.

12. An arrangement according to claim **7**, characterized in that the boundary is not established until agreement is found with regard to a predetermined number of mutually sequential data packets.

13. An arrangement according to claim **8**, characterized in that the boundary is not established until agreement is found with regard to a predetermined number of mutually sequential data packets.

14. An arrangement according to claim **4**, characterized in that when no agreement is found with any of the incoming connections (**2***a*–**2***d*), the predetermined part of a consecutive bit sequence is moved one bit position forwards or

backwards, whereafter a check calculation is carded out on said part in the same way as earlier, so as to establish the boundary when agreement is found and so as to move the predetermined part through a further bit position in the same direction when no agreement is found.

15. An arrangement according to claim 9, characterized in that when no agreement is found with any of the incoming connections (2*a*–2*d*), the predetermined part of a consecutive bit sequence is moved one bit position forwards or backwards, whereafter a check calculation is carded out on said part in the same way as earlier, so as to establish the boundary when agreement is found and so as to move the predetermined part through a further bit position in the same direction when no agreement is found.

16. An arrangement according to claim 10, characterized in that when no agreement is found with any of the incoming connections (2*a*–2*d*), the predetermined part of a consecutive bit sequence is moved one bit position forwards or backwards, whereafter a check calculation is carried out on said part in the same way as earlier, so as to establish the boundary when agreement is found and so as to move the predetermined part through a further bit position in the same direction when no agreement is found.

17. An arrangement according to claim 11, characterized in that when no agreement is found with any of the incoming connections (2*a*–2*d*), the predetermined part of a consecutive bit sequence is moved one bit position forwards or backwards, whereafter a check calculation is carried out on said part in the same way as earlier, so as to establish the boundary when agreement is found and so as to move the predetermined part through a further bit position in the same direction when no agreement is found.

18. An arrangement according to claim 12, characterized in that when no agreement is found with any of the incoming connections (2*a*–2*d*), the predetermined part of a consecutive bit sequence is moved one bit position forwards or backwards, whereafter a check calculation is carried out on said part in the same way as earlier, so as to establish the boundary when agreement is found and so as to move the predetermined part through a further bit position in the same direction when no agreement is found.

19. An arrangement according to claim 13, characterized in that when no agreement is found with any of the incoming connections (2*a*–2*d*), the predetermined part of a consecutive bit sequence is moved one bit position forwards or backwards, whereafter a check calculation is carded out on said part in the same way as earlier, so as to establish the boundary when agreement is found and so as to move the predetermined part through a further bit position in the same direction when no agreement is found.

* * * * *

US005432785A

United States Patent [19]

Ahmed et al.

[11] Patent Number: 5,432,785

[45] Date of Patent: Jul. 11, 1995

[54] **BROADBAND PRIVATE VIRTUAL NETWORK SERVICE AND SYSTEM**

[75] Inventors: **Masuma Ahmed**, Middletown; **Stephen M. Walters**, Holmdel, both of N.J.

[73] Assignee: **Bell Communications Research, Inc.**, Livingston, N.J.

[21] Appl. No.: **192,763**

[22] Filed: **Feb. 7, 1994**

Related U.S. Application Data

[63] Continuation of Ser. No. 964,330, Oct. 21, 1992, abandoned.

[51] **Int. Cl.**[6] **H04J 3/24**; H04Q 11/04

[52] **U.S. Cl.** **370/60.1**; 370/94.2

[58] **Field of Search** 370/15, 16, 54, 58.1, 370/58.2, 58.3, 60, 60.1, 94.1, 94.2, 110.1, 112

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,050,162	9/1991	Golestani	370/60
5,067,123	11/1991	Hyodo et al.	370/94.1
5,115,427	5/1992	Johnson, Jr. et al.	370/60
5,119,369	6/1992	Tanabe et al.	370/60
5,177,736	1/1993	Tanabe et al.	370/15
5,224,092	6/1993	Brandt	370/94.1
5,239,537	8/1993	Sakauchi	370/16
5,265,088	11/1993	Takigawa et al.	370/15

OTHER PUBLICATIONS

"A new Direction for Broadband ISDN", Stephen Walters, IEEE, Sep. 1991, pp. 39–42.

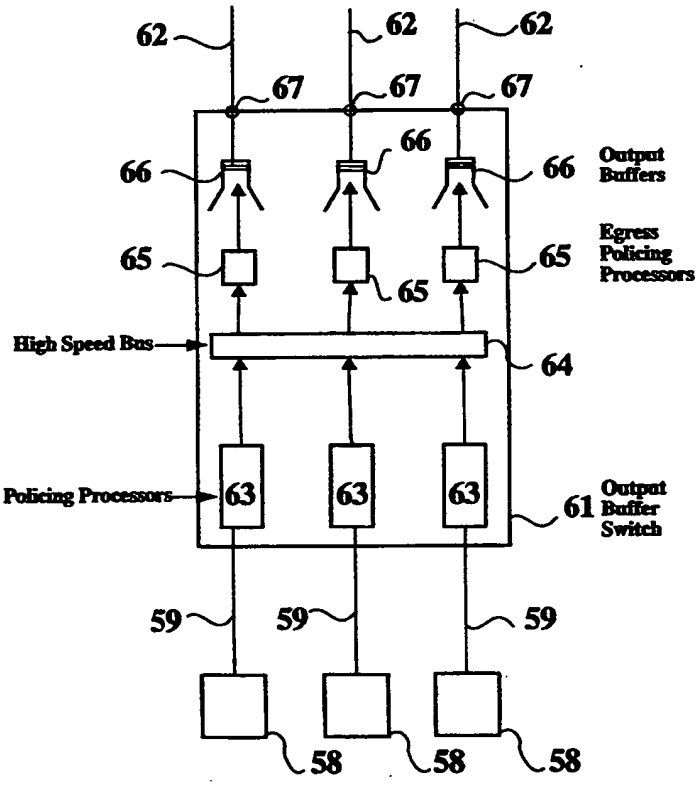
Primary Examiner—Alpus Hsu

Attorney, Agent, or Firm—Leonard Charles Suchyta; Joseph Giordano

[57] **ABSTRACT**

A system and method for operating a Broadband ISDN to support a viable virtual private network (VPN) service are attained by establishing a plurality of virtual path links connecting customer locations and broadband switching systems, by cross-connecting virtual channel links at the broadband switching systems to establish end-to-end virtual channel connections, and by policing both the input and output traffic only on the virtual path links. An egress policing processor is included at each output port on broadband switches to police the traffic on each virtual path link which contains one customer's multiplexed virtual channel connection traffic.

7 Claims, 9 Drawing Sheets



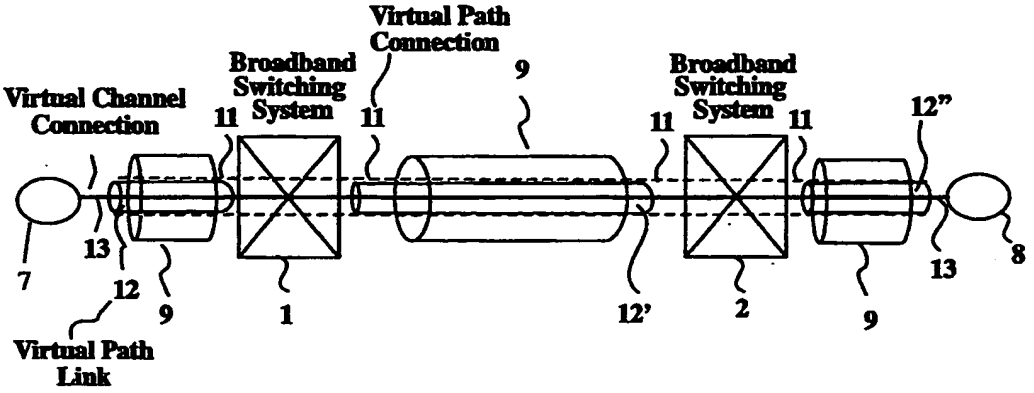


FIGURE 1
(Prior Art)

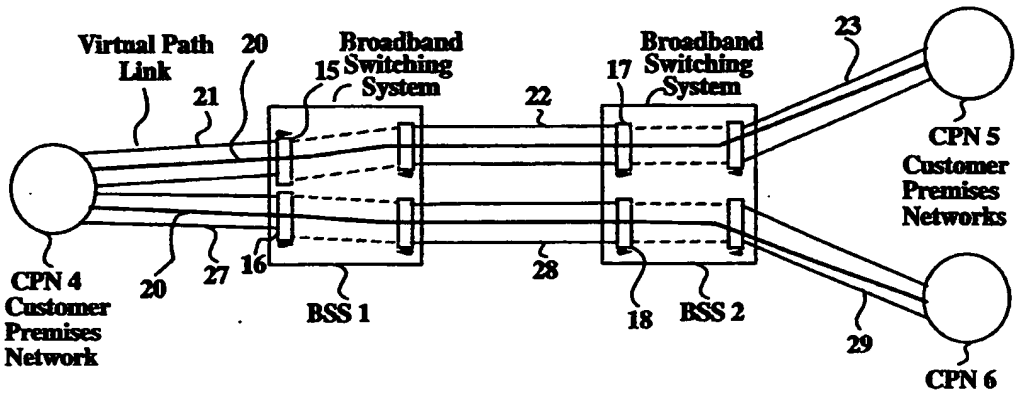


FIGURE 2

(Prior Art)

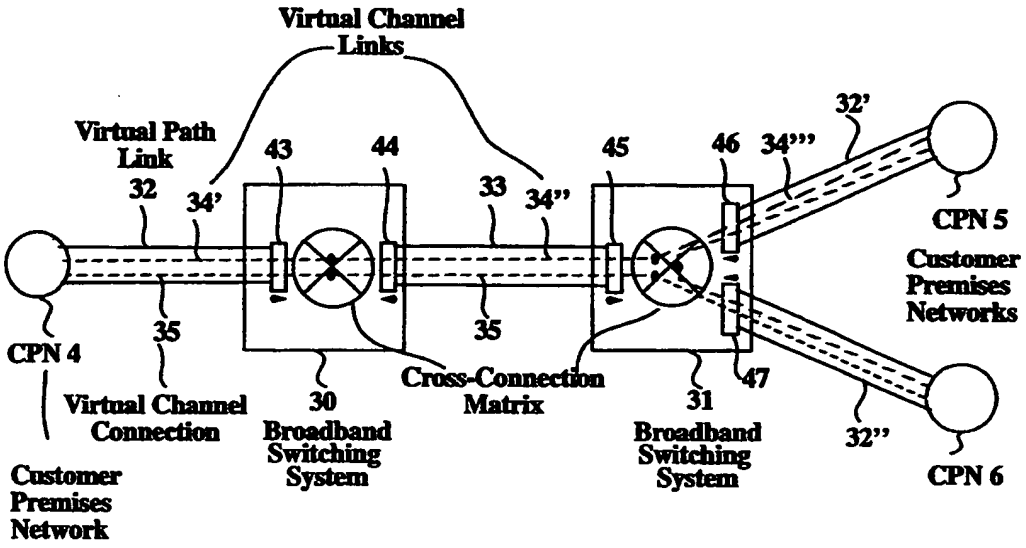

Virtual Channel Links
Virtual Path Link
32
34'
43
44
33
34''
45
46
34'''
32'
CPN 5
Customer Premises Networks
CPN 4
35
35
Virtual Channel Connection
30
Broadband Switching System
Cross-Connection Matrix
31
47
Broadband Switching System
32''
CPN 6
Customer Premises Network

FIGURE 3

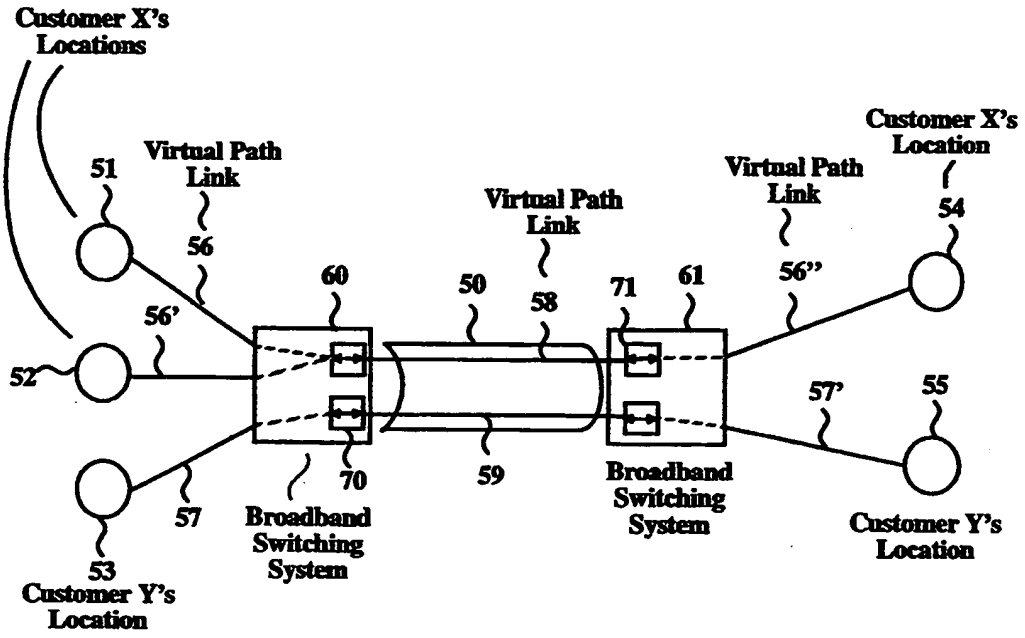

Customer X's Locations
Virtual Path Link
51
56
56'
52
60
50
58
Virtual Path Link
71
61
Virtual Path Link
56''
Customer X's Location
54
57'
55
57
53
Customer Y's Location
Broadband Switching System
70
59
Broadband Switching System
Customer Y's Location

FIGURE 4

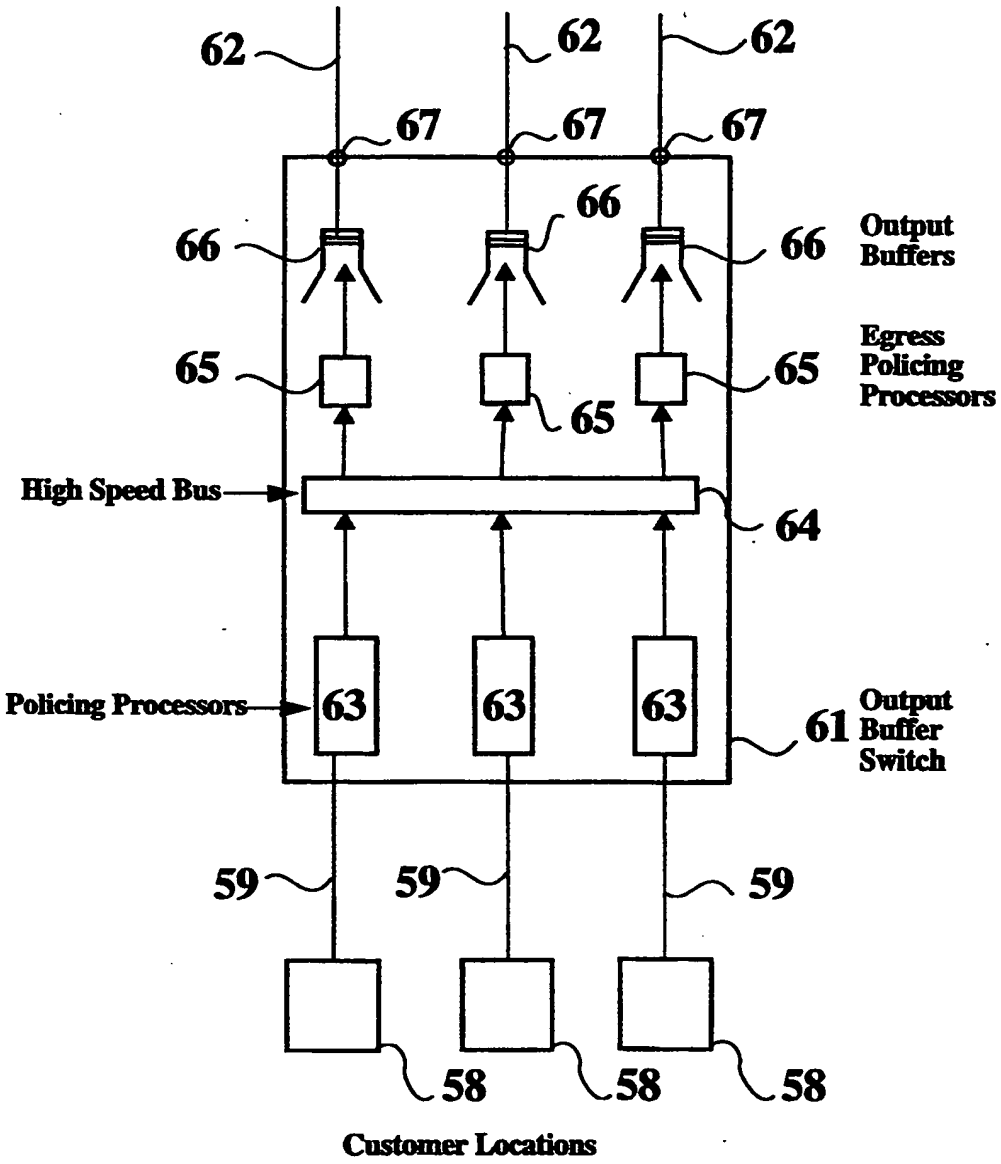

62
62
62
67
67
67
66
66
66
Output Buffers
65
65
65
Egress Policing Processors
High Speed Bus
64
Policing Processors
63
63
63
61
Output Buffer Switch
59
59
59
58
58
58
Customer Locations

FIGURE 5

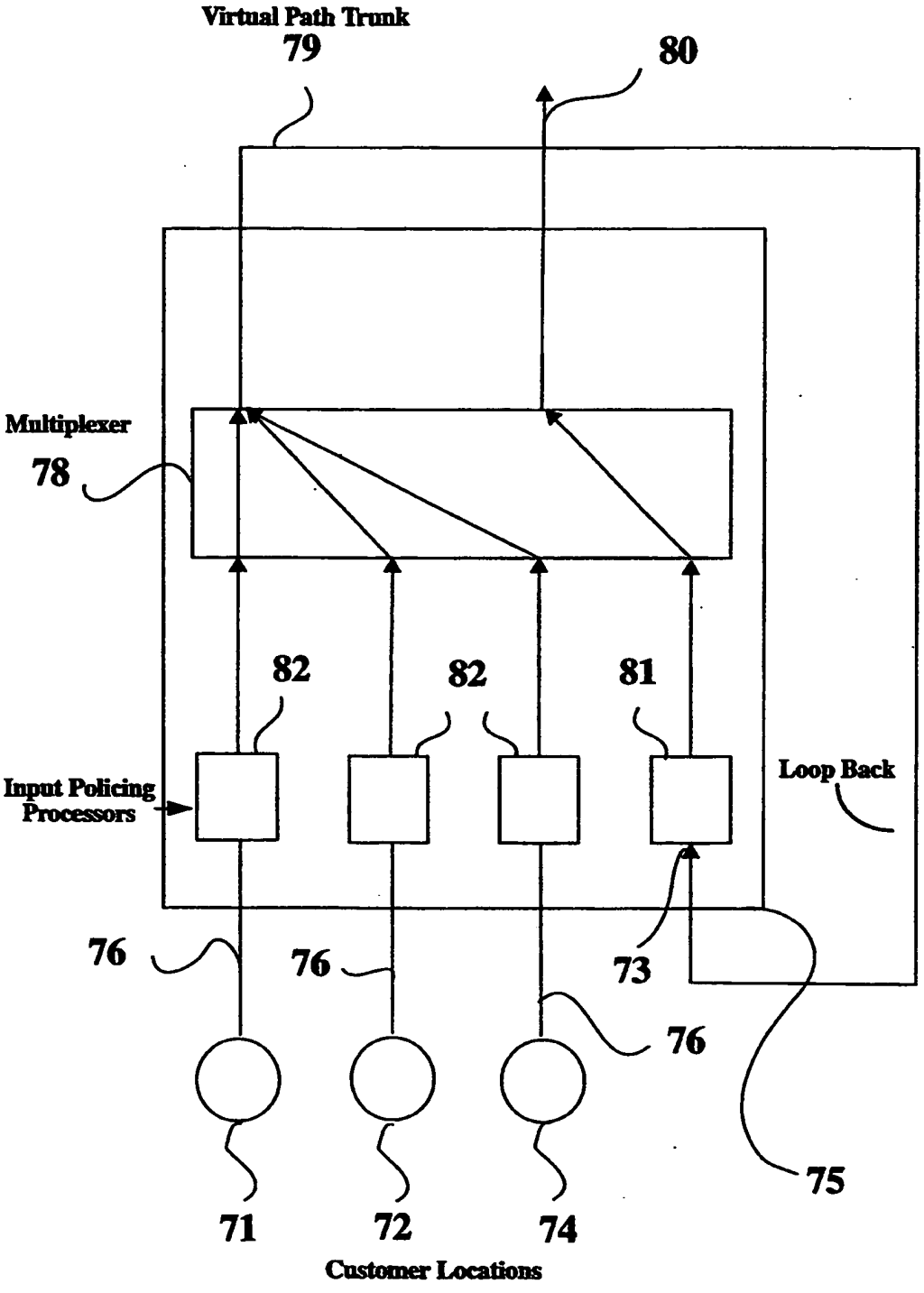

Virtual Path Trunk
79
80
Multiplexer
78
82
82
81
Input Policing Processors
Loop Back
76
76
73
76
75
71
72
74
Customer Locations

FIGURE 6

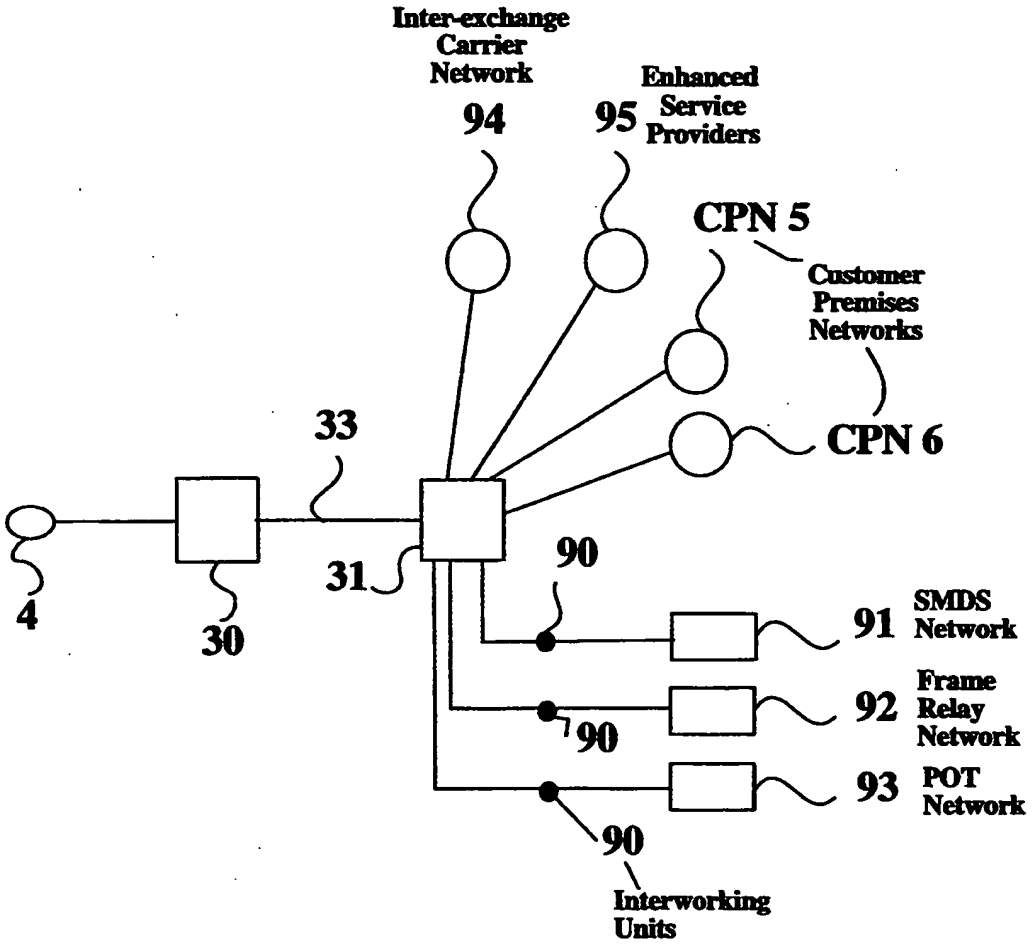

Inter-exchange Carrier Network
94
95
Enhanced Service Providers
CPN 5
Customer Premises Networks
CPN 6
33
4
30
31
90
91
SMDS Network
92
Frame Relay Network
90
93
POT Network
90
Interworking Units

FIGURE 7

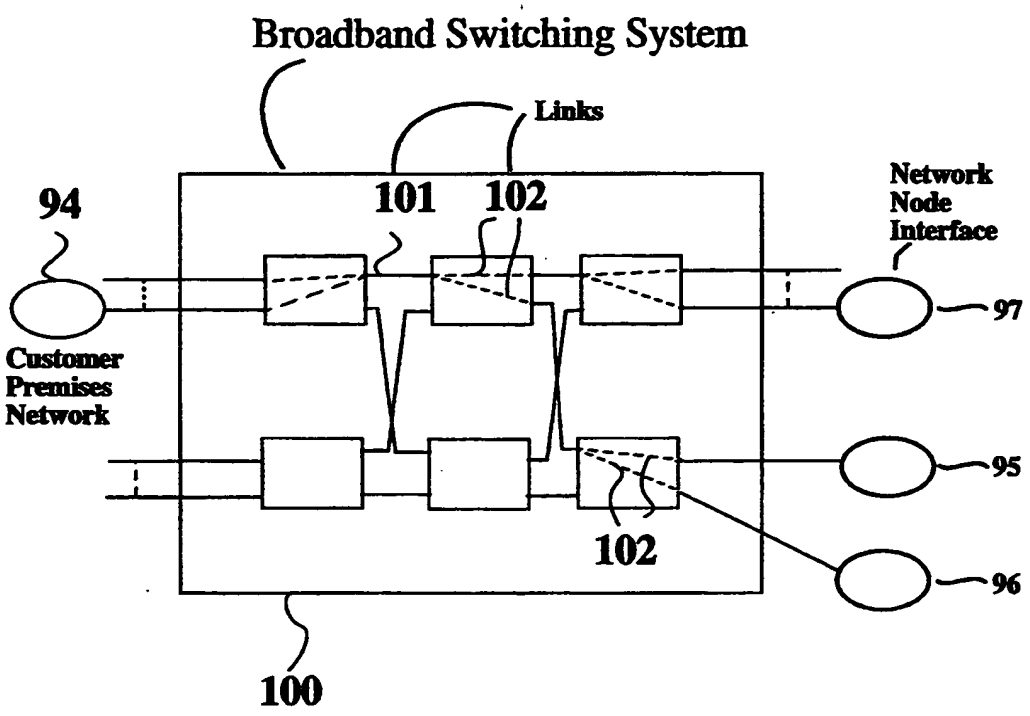

Broadband Switching System
Links
101
102
94
Network
Node
Interface
97
Customer
Premises
Network
95
102
96
100

FIGURE 8

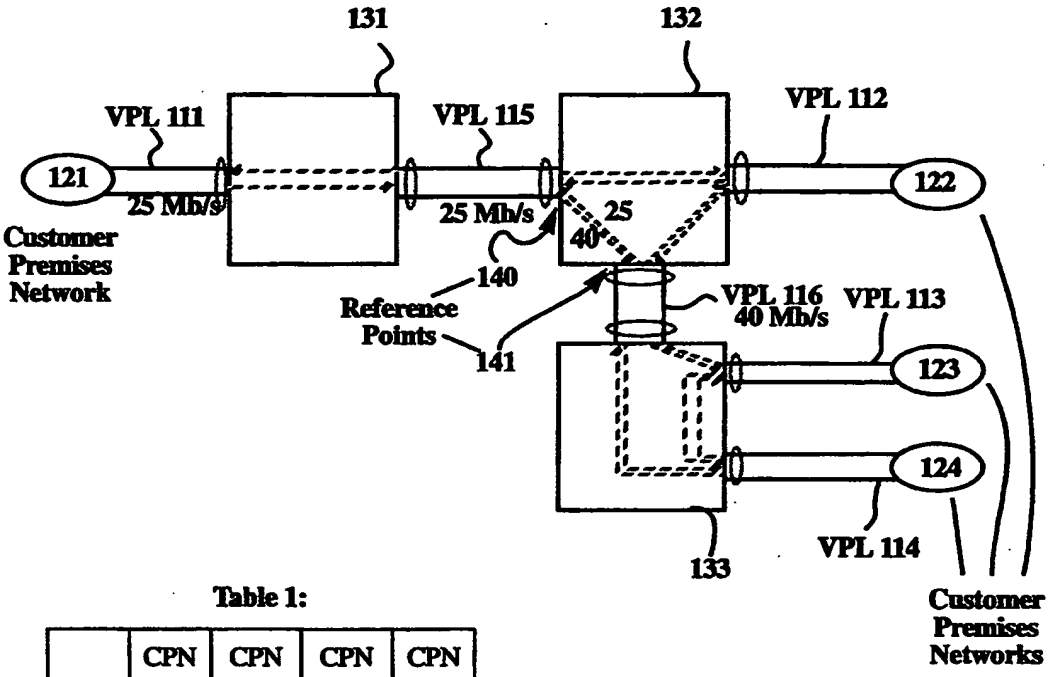


Table 1:

	CPN 121	CPN 122	CPN 123	CPN 124
CPN 121		3,15	5,15	5,10
CPN 122	3,15		10,15	5,10
CPN 123	5,15	10,15		5,20
CPN 124	5,10	5,10	5,20	

FIGURE 9

BROADBAND PRIVATE VIRTUAL NETWORK SERVICE AND SYSTEM

This application is a continuation of application Ser. No. 07/964,330 filed on Oct. 21, 1992, now abandoned.

CROSS REFERENCE TO RELATED APPLICATIONS

This patent application is related to U.S. patent application Ser. No. 07/964,332 entitled "System and Method for Providing Egress Policing for Broadband Virtual Private Networks" by Ahmed et al., bearing attorney docket number 646, and filed on the same date as this application, now abandoned.

TECHNICAL FIELD OF THE INVENTION

This invention relates to a broadband communication service and system and more specifically to a new Broadband Virtual Private Network (BVPN) service, and a system for providing such a service.

BACKGROUND OF THE INVENTION

Over the last few years the telecommunications industry has devoted a considerable amount of work and time toward defining the capabilities of Broadband ISDN (B-ISDN). The goal has been to match transport capabilities available in B-ISDN to potential user applications. Examples of such user applications are accessing remote data bases with very low latency, transmitting large multimedia files containing photographic quality images and/or video snipets, and performing desktop multimedia teleconferencing including video. All of these applications demand high-speed transmission and switching within the interconnection network and many require new signaling capabilities beyond that of the current ISDN signaling protocol Q.931.

However, many people knowledgeable about the network recognize that the time-frame necessary to deploy all of these capabilities is well into the future; therefore it is believed that this feature-rich B-ISDN technology is still years away. Accordingly, there is a market opportunity for a broadband service that can be quickly and inexpensively deployed. Such a market opportunity can be met with a virtual private network capability deployed within the B-ISDN public network.

B-ISDN is characterized by the transport of Asynchronous Transport Mode (ATM) cells over ATM connections. ATM cells are fixed length packets which contains addressing and transmission instructions along with user data. This allows ATM cells to be independently addressed and transmitted on demand over ATM connections facilitating transmission bandwidth to be allocated, as needed, without fixed hierarchical channel rates. ATM connections are set-up between various nodes in the network and also between the customer premises equipment and the network nodes. ATM connections are organized in two levels: virtual channels (VCs) and virtual paths (VPs). End-to-end virtual channel connections are made up from virtual channel links which are switched or cross-connected at the broadband switching systems. Virtual channel links are carried within virtual path links which in turn are switched or cross-connected to form end-to-end virtual path connections. The virtual channel identifier (VCI) and virtual path identifier (VPI) fields in the ATM cell header identify the virtual channel link and the virtual path link to which the ATM cells belong. Multiple virtual channel links (of varying bandwidths) can be grouped into virtual path links and multiple virtual channel links and virtual path links can be carried on a physical link. Virtual channel connections and virtual path connections are bi-directional with either symmetric or asymmetric cell transfer capability.

One of the basic characteristics of ATM networks is the provisioning of ATM traffic parameters at the user-network access interfaces (UNIs) and the network-node interfaces (NNIs). The ATM traffic parameters describe the traffic characteristics such as cell transfer rate and quality of service of an ATM connection (which can be a virtual channel connection or a virtual path connection). Traffic parameters include, but are not limited to, peak cell transfer rate, average cell transfer rate, and burst length. Currently, only peak cell transfer rate has been standardized into CCITT I.371 1992 recommendations. Even though a customer can contract for a peak cell transfer rate on an ATM connection, in principle, the user could exceed the negotiated traffic parameter up to the maximum capacity of the physical facility. Therefore, a network function called "usage parameter control" or "policing" as defined in CCITT recommendation I.311. is needed. This function controls the cell stream during the entire active phase of the ATM connection and restricts the peak traffic to the characteristics negotiated in the contract. Thus, it will protect the network against excessive congestion resulting in a degradation of the quality of service of all connections sharing the same network resources.

To protect all network resources, the policing function is located as close as possible to the actual traffic source and is under the control of the network providers. Depending on the service being provided, the policing function may be performed on virtual channel links or on virtual path links. The prior art policing function is performed at the ingress of the broadband switching systems at both the user-network interfaces and the network-node interfaces. To protect the network and the coexisting connections, actions must be taken by the policing function after detecting a violation of the contract. The prior art policing action is to discard those cells which are in violation of the traffic contract. Other policing actions, such as marking the violating cells as low priority cells and discard them only during network congestion, are being discussed in the art.

The prior art B-ISDN allows for the deployment of Virtual Private Network (VPN) services by either cross-connecting virtual channel links (Virtual Channel Cross-connect (VCX) functionality) or cross-connecting virtual path links (Virtual Path Cross-connect (VPX) functionality). In the prior art B-ISDN, when cross-connecting virtual channel links, policing is accomplished on the traffic on the virtual channel links. Similarly, when cross-connecting virtual path links, the policing is accomplished only on the traffic carried on the virtual path links. Therefore, when using VPX or VCX functionality to deploy Virtual Private Networks, ATM connections and its bandwidth (peak cell transfer rate) are directly coupled. As a result, as the number of customer locations and therefore the number of desired connections in a VPN increases, the transmission capacity needed on the physical facilities must increase to support the cumulative bandwidth of all the connections on the facility even though all the connections would never be simultaneously active with traffic at their peak bandwidth. This excess provisioning of transmission capacity can cause the whole concept of virtual

private networks (VPNs) to fail. Therefore, a primary objective of our invention is to provide a viable private network capability by separating bandwidth from connectivity requirements.

SUMMARY OF THE INVENTION

Our invention is a system and method for operating a Broadband ISDN to support a viable virtual private network (VPN) service. This is accomplished by establishing a plurality of virtual path links connecting customer locations and broadband switching systems, by cross-connecting virtual channel links at the broadband switching systems to establish virtual channel connections, and by policing both the input and output traffic only on the virtual path links. Therefore, the individual virtual channel link bandwidth is not policed and the traffic on any virtual channel link can periodically reach, as needed, the peak cell transfer rate of the virtual path link which contains it, thereby uncoupling the bandwidth from the connection. However, to support multiple VPNs in a public network, it is required to police traffic on the virtual path links at the egress of the broadband switching systems in order to protect the quality of service of each VPN. Therefore, an additional aspect of our invention is to include a policing processor on the output ports of the broadband switching systems for each virtual path link.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 depicts the relationship between a virtual paths and virtual channels in a Broadband ISDN.

FIG. 2 illustrates the prior art virtual path connections and virtual channel connections in Broadband ISDN.

FIG. 3 depicts an illustrative embodiment of our inventive service architecture.

FIG. 4 depicts an embodiment of our invention when two private virtual networks share facilities.

FIG. 5 illustrates egress policing on an output buffer type switch.

FIG. 6 depicts our method for providing egress policing using a loopback of grouped traffic into a broadband switching system input port.

FIG. 7 illustrates an extension of our BVPN.

FIG. 8 illustrates resource allocation within a broadband switching system.

FIG. 9 depicts an example of resource allocation within our BVPN.

DETAILED DESCRIPTION

The relationships between a virtual path, a virtual channel, the physical facility, and the network elements must be clearly understood to facilitate a detailed description of our invention. FIG. 1 illustrates these relationships. A virtual channel connection 13 is an end-to-end connection between customer premises network 7 and 8 contained, exclusively, within virtual path connection 11. The virtual path connection 11 is established by cross-connecting virtual path links 12 and 12' at broadband switching system 1 and by cross-connecting virtual path links 12' and 12'' at broadband switching system 2. The virtual path links and virtual channel connections are both carried within physical facilities 9.

FIG. 2 depicts a prior art B-ISDN providing virtual private network (VPN) services using virtual path connections. Three customer premises networks, customer premises network 4, customer premises network 5 and customer premises network 6, are connected to form a customer's VPN using VPX functionality. Customer premises network 4 and customer premises network 5 are connected by a virtual path connection which was established by cross-connecting at the broadband switching system 1 virtual path link 21 and virtual path link 22, and by cross-connecting at broadband switching system 2 virtual path link 22 and virtual path link 23. Customer premises network 4 and customer premises network 6 are connected by virtual path connection, which was established by cross-connecting at broadband switching system 1 virtual path link 27 and virtual path link 28, and by cross-connecting at broadband switching system 2 virtual path link 28 and virtual path link 29. Within each virtual path connection, the customer can set-up multiple virtual channel connections which are transparent to broadband switching system 1 and broadband switching system 2. It is important to note that in the prior art B-ISDN providing VPN services, an entire virtual channel connection must be contained within and coincident with a virtual path connection. An example virtual channel connection 20 is shown as contained within the virtual path connection established between customer premises networks 4 and 5. Ingress policing on the originating traffic from customer premises network 4 carried by virtual path link 21 and virtual path link 27 is accomplished at the user-network access interfaces by policing processor 15 and policing processor 16, respectively at broadband switching system 1. Ingress policing on the incoming traffic originating from customer premises network 4 carried by virtual path link 22 and virtual path link 28 is accomplished at the network-node interfaces at broadband switching system 2 by policing processor 17 and policing processor 18, respectively. (Note: the arrows shown in FIG. 2 depict the traffic direction on which the policing processor operates). These are the only four places where the traffic originating from customer premises network 4 is policed. In this architecture, bandwidth and connectivity (i.e. virtual path bandwidth and virtual path connections) are directly coupled which is a fundamental problem in using this prior art B-ISDN architecture for providing VPN services.

To illustrate the problem, let us assume that each customer premises network in the example VPN is a 10 Mb/s LAN. Therefore at any instant of time, each customer premises network in the example VPN can transmit or receive ATM cells up to the 10 Mb/s rate. As a result, the virtual path connections between networks 4 and 5 and networks 4 and 6 both have to be provisioned to support a peak bit rate of 10 Mb/s, each. Therefore, the physical facility between customer premises network 4 and broadband switching system 1 must be provisioned to support at least 20 Mb/s (10 Mb/s for each virtual path link) even though customer premises network 4 has a maximum transmission capability of only 10 Mb/s. As the number of customer locations in a VPN increases, for example to 20 locations, the transmission capacity needed on the physical facility between customer premises network 4 and broadband switching system 1 for example, must be capable of supporting a transmission rate of 190 Mb/s (10 Mb/s for 19 virtual path links to accommodate 19 virtual path connections) even though customer premises network 4 can receive and transmit at only 10 Mb/s. This excessive provisioning of the transmission capacity makes the whole concept of virtual private networks (VPNs) in the prior art technically not viable and completely uneconomical.

The service architecture of our Broadband Virtual Private Network (BVPN) which eliminates the excessive provisioning of transmission capacity problem described above is depicted in FIG. 3. Individual virtual path links 32, 32' and 32" connect each of the customer premises networks 4, 5 and 6 to a broadband switching system 30 and 31. A virtual path link 33 also connects broadband switching system 30 to broadband switching system 31. Virtual path links 32, 32', 32" and 33 belong to one customer and carry only that customer's traffic. However, in comparison to the prior art B-ISDN, the virtual path links in our invention are not connected into a virtual path connection and each of the virtual path links 32, 32', 32" and 33 may have different traffic characteristics. Furthermore, our network establishes virtual channel connections by cross-connecting virtual channel links at each broadband switching system. The virtual channel links are established within the virtual path links. For example, within virtual path link 32 connecting customer premises network 4 to broadband switching system 30 is virtual channel link 34', within virtual path link 33 connecting broadband switching system 30 and broadband switching system 31 is virtual channel link 34", and within virtual path link 32' connecting broadband switching system 31 and customer premises network 5 is virtual channel link 34"'. Each broadband switching system then cross-connects the virtual channel links to establish the end-to-end connection. In this architecture, only the virtual channel connections have end-to-end capability and the aggregate traffic on the virtual channel connections are controlled at the ingress on the virtual path links using policing processors 43, 44, 45 and 46. Again, the arrows depict the traffic direction on which the policing processors operate. Policing processor 43 manages the traffic on the virtual path link 32 to within contracted parameter values. The traffic on the virtual channel connection is not policed. In this way, a completely arbitrary number of connections to any number of locations may be provided but without fixing their individual bandwidth. This allows connectivity and bandwidth to be specified independently.

A second aspect our invention addresses the problem of multiple customers in a BVPN affecting each others service performance as would be experienced in the prior art architecture, again consider FIG. 3 with each customer premises network being a 10 Mb/s LAN. Since, the customer premises network 4 can only transmit and receive, in aggregate, at a 10 Mb/s rate, and since virtual channel connections can be established to the other two locations using only a single virtual path link on the access facility, virtual path link 32 need only be provisioned to support a maximum traffic load of 10 Mb/s. In the prior art, each set of virtual channel connections to different customer locations required their own virtual path and consequently their own virtual path link on the access facility thereby, requiring the access facility to be provisioned to support 20 Mb/s.

Since the equipment supporting our BVPN can be shared by several different customers, a single physical network is cost effective and attractive to customers provided that the various BVPNs do not interfere with each other. To prevent this interference, traffic management capabilities (i.e. policing) is introduced in the network to prevent one user's excess traffic from degrading the quality of service available to another B-ISDN customer. The needed traffic management capabilities place special requirements on the broadband switching systems to provide the BVPN.

Consider the simple network depicted in FIG. 4 which illustrates our BVPN service on a B-ISDN with users sharing B-ISDN resources. A customer X has three locations 51, 52, and 54 connected in one virtual private network. A second customer Y has two locations 53 and 55 connected in a second virtual private network. Each of customer's X's locations has established a 50 Mb/s virtual path link 56, 56' and 56" to one of the broadband switching systems 60 and 61, while each of customer Y's locations has established a 100 Mb/s virtual path link 57 and 57' to one of the broadband switching systems 60 and 61. Additionally, customer X has established a 50 Mb/s virtual path link 58 on transmission facility 50, while customer Y has established a 100 Mb/s virtual path link 59 on transmission facility 50. Customer X can set up multiple virtual channel connections between its locations. Thus, customer X's location 51 could send up to 50 Mb/s to customer X's location 54 one virtual channel connection while customer X's location 52 can also send up to 50 Mb/s to customer X's location 54.

Current art broadband switching systems limit the input traffic they receive from customer access lines to a negotiated value using a policing processor (referred to in the art as a Usage Parameter Control (UPC) device) on the input side of the network. In order for customer X and Y to share the interoffice facility 50, policing the outgoing traffic on each customer's interoffice virtual path links is necessary (i.e. egress policing). The need for egress policing is due to the fact that when customer X transmits 50 Mb/s simultaneously from locations 51 and 52, 100 Mb/s is transmitted on virtual path link 58. With the interoffice facility only capable of 150 Mb/s and with customer X causing 100 Mb/s traffic on virtual path link 58, customer X is effectively leaving customer Y with only 50 Mb/s bandwidth thereby affecting customer Y's quality of service. Therefore, it is a second aspect of our invention to provide an egress policing processor at the output of each broadband switching system for each virtual path link. Our inventive architecture provides for a policing processor on the output port of the broadband switching systems for each virtual path link. Egress policing processors 70 are depicted in FIG. 4 with the arrows indicating the direction of the traffic that is policed. The policing processors have arrows pointing both ways to indicate that the traffic is policed in both directions: on the input as ingress policing used in the prior art, and on the output as egress policing as disclosed herein. The realization of egress policing is dependent on the broadband switching system architecture.

There are three major implementation architectures for broadband switches. These are: input buffer type, shared buffer type, and output buffer type. In our preferred embodiment we disclose egress policing on an output buffer type switch, although the inventive concept is equally applicable to the other two switch architectures. FIG. 5 illustrates such an embodiment. In the output buffer type switch 61, all input cells from customer's networks 58 on customer's access lines 59 are policed at a policing processor 63 on a negotiated value. All cells that pass through the policing processors 63 are multiplexed on a high-speed internal bus 64. Cells on the internal bus 64 are directed toward an appropriate output port 67 and stored in a buffer 66 equipped to each output port. In a typical prior art output buffer

switch, the output buffer is shared by many virtual paths and virtual channels. To realize egress policing, policing processors **65** are placed between the internal bus **64** and the output buffers **66** which are then segregated and dedicated to each virtual path link **62** at output port **67**.

An alternative embodiment, as set forth in the above cited Ahmed et al. patent application, does not require the introduction of a policing processor at the output port of the broadband switching systems. The point of our BVPN is to use transmission facilities efficiently. FIG. **6** shows this alternative embodiment. In this architecture, traffic from customer locations **71** and **72** over access lines **76** are policed by ingress policing processors **82** and then are multiplexed at multiplexor **78** into a virtual path trunk line **79**. This trunk line does not require a special trunk circuit, but is physically looped back to input port **73** of broadband switching system **75**. At input port **73**, an ingress policing processor **81**, similar to the policing processors **82** at all the input ports, is used to provide the desired egress policing function i.e. to police the aggregated traffic to a negotiated virtual path link transmission capacity. The multiplexed traffic can then be combined with the traffic from another customers' location **74** for transport on physical facility **80**.

In this switch architecture, extra switching ports and capacity are needed. The maximum number of extra switching ports is equal to the total number of outgoing virtual path links used for the BVPN. However, the actual number of extra ports needed for the broadband switching systems may be less than this maximum. If the aggregated input capacity is equal to or less than an output virtual path link capacity, the output virtual path link can be directly multiplexed with other customers' traffic on the same physical transmission link. In this case, the extra port is unnecessary.

As shown in FIG. **3** and FIG. **4**, our BVPN simply interconnects the customer's locations. The result is an island network which does not allow traffic to be routed outside the private network and provides only point-to-point connections. However, various extensions could be provided. These are shown in FIG. **7**. There the basic BVPN, connecting customer premises networks **4**, **5**, and **6** via broadband switching systems **30** and **31**, has been supplemented with interworking units **90** for access to any pre-existing services, such as Switched Multimegabit Services (SMDS) **91**, Frame Relay Service **92**, or Plain Old Telephone Service (POTS) **93**. It could also support access to Inter-Exchange Carder (IEC) **94** service providers or to Enhanced Service Providers (ESP) **95**.

In our BVPN network, the bandwidth of the virtual channel connections in a virtual path link can vary with time, and at any instant of time, the bandwidth of a virtual channel connection can equal the peak capacity of the virtual path link. Therefore, the virtual channel connections established between the input and output ports in a broadband switching system are required to transport any cell transfer rate up to the peak capacity of its virtual path links. This requirement on virtual channel connection cell transfer rate increases the required capacity of a broadband switching system. It is another aspect of our invention to optimize broadband switching system resource allocation. FIG. **8** depicts one method for resource allocation. In the figure, the virtual channels from customer premises network **94** destined to customer premises network **95**, customer premises network **96** and the Network-to-Node interface (NNI) **97** through our broadband switching network **100**, would go through the same link **101** until it is necessary to fan them out on separate links **102**.

An example of BVPN traffic matrix with BVPN resource allocation is illustrated in FIG. **9**. For the purpose of the analysis, the traffic flow between any two customer premises network locations is assumed to be bidirectional and symmetric. The virtual path link capacities at the access could be estimated as follows:

$$R_{peak}(VPL111) = \sum_{122}^{124} R_{min}(121, j) + \max\Delta R(121, j), j = 122, 123, 124)$$

where:

$$\Delta R(i,j) = R_{max}(i,j) - R_{min}(i,j)$$

$R_{min}(i,j)$=minimum traffic capacity between customer locations i and j

$R_{max}(i,j)$=maximum traffic capacity between customer locations i and j

Thus, the peak traffic capacity for virtual path link **111** can be calculated using the expected minimum and maximum traffic between customer locations as shown in Table 1. Each ordered pair in Table 1 depicts the minimum and maximum traffic, respectively, between the labeled customer premises networks (CPNs). As shown, the minimum traffic between CPN **121** and CPN **122** is 3 Mb/s, between CPN **121** and CPN **123** is 5 Mb/s, and between CPN **121** and CPN **124** is 5 Mb/s. Using the equation above, the expected peak traffic capacity for virtual path link **111** is calculated by first summing the minimum values (equaling 13 Mb/s) and then adding that sum to the maximum of the difference between the minimum and maximum expected traffic between CPN **121** and the other CPNs. In this case the maximum of the difference is 12 Mb/s which is the difference between the minimum and maximum traffic expected between CPN **121** and CPN **122**. Therefore the peak traffic allocation for virtual path link **111** is 25 Mb/s (the 13 Mb/s sum plus the 12 Mb/s maximum difference).

As disclosed earlier, the bandwidth of the virtual channel connections within a virtual path link can vary with time and therefore could increase the internal capacity of a virtual channel cross-connect capability within a broadband switching system. The equation above can be used to determine the peak traffic between any two input and output ports. Furthermore, the virtual channel cross-connected within a broadband switching systems are bidirectional but do not necessarily have symmetric capabilities. For example, as shown in FIG. **9**, the peak capacity allocated to virtual channels going from reference point **140** to reference point **141** is 25 Mb/s, whereas peak capacity allocated to the same virtual channels in the opposite direction is 40 Mb/s. Also, note that the combined traffic from customer premises network **122**, customer premises network **123**, and customer premises network **124** destined for virtual path link **115** could exceed its peak capacity, 25 Mb/s, if the outgoing traffic is not policed.

It is to be understood that the system and method for providing Broadband Virtual Private Network Service on a Broadband ISDN public network illustrated herein are not limited to the specific forms disclosed and illus-

trated, but may assume other embodiments limited only by the scope of the appended claims.

We claim:

1. A broadband system for providing a virtual private network capability to customers each having a plurality of locations and comprising:

a plurality of broadband switching systems each having input and output ports;

a plurality of virtual path links connecting said customer locations to one of said broadband switching systems and connecting any two of said broadband switching systems;

a plurality of virtual channel links contained within said virtual path links;

virtual channel connections between any two of said plurality of customer locations established by cross-connecting said virtual channel links at said broadband switching systems;

means for policing incoming traffic on said virtual path links at said input ports on said broadband switching systems; and

means for policing outgoing traffic on said virtual path links at said output ports of said broadband switching systems.

2. A broadband system as recited in claim 1 wherein each of said plurality broadband switching systems comprise:

means for multiplexing all traffic from a plurality of one customer's locations into one of said virtual path links.

3. A broadband system as recited in claim 2 wherein said means for policing incoming traffic and means for policing outgoing traffic on said virtual path links each comprises:

means for regulating traffic on said multiplexed virtual channel connections wherein a customer may transmit on any virtual channel the peak bandwidth allocation for any of said virtual path links without affecting the service provided to other customers.

4. A broadband ISDN system for providing a virtual private network capability comprising:

at least one broadband switching system further comprising

a plurality of input/output ports,

means for cross connecting virtual channel links between one of said input/output ports and another of said input/output ports to establish end-to-end virtual channel connections,

means for policing the incoming traffic on a first virtual path link at said input ports,

means for policing the outgoing traffic on a second virtual path link at said output ports, and

a broadband access line from each of a plurality of customer locations to any one of said broadband switching systems;

a plurality of virtual path links containing a plurality of one customers' virtual channel links on said broadband access line connecting said customer locations; and

a plurality of virtual channel connections established between said customer locations by said means for cross-connecting where the combined outgoing traffic of one customer's virtual channel connections is policed by said outgoing traffic policing means on said first virtual path link, and where one customer's combined incoming traffic from that customer's virtual channel connections on said second virtual path link is policed by said incoming traffic policing means.

5. A method for operating a broadband ISDN having a plurality of broadband switching systems and broadband transport facilities for providing a customer a broadband private virtual network service, said method comprising the steps of:

providing the customer with the capability to establish virtual channel connections by cross-connecting virtual channel links at said broadband switching systems between a plurality of customer locations;

establishing virtual path links containing said virtual channel links between said customer locations and said broadband switching systems, and between said broadband switching systems;

multiplexing said virtual channel connections together at each of said broadband switching systems for routing over said virtual path links,

policing the incoming traffic on said virtual path links at input ports on said broadband switching systems; and

policing the outgoing traffic on said virtual path links at output ports on said broadband switching system.

6. The method as recited in claim 5 wherein said step of policing the incoming traffic and said step of policing outgoing traffic further comprises:

limiting the total traffic volume on each of said virtual path links below some specified threshold independently established for each of said virtual path links.

7. The method as recited in claim 6 wherein said traffic on said broadband switching systems is comprised of ATM cells and wherein said limiting the traffic volume step comprises:

discarding those ATM cells which exceed said specified threshold.

* * * * *

HPS Trailer Page
for
EAST

UserID: VNguyen7_Job_1_of_1

Printer: cpk2_3b05_gbxaptr

Summary

Document	Pages	Printed	Missed	Copies
US005432785	15	15	0	1
Total (1)	15	15	0	-

US005513178A

United States Patent [19]

Tanaka

[11] Patent Number: 5,513,178

[45] Date of Patent: Apr. 30, 1996

[54] **CELL MULTIPLEXING APPARATUS IN ATM NETWORK**

[75] Inventor: **Kenji Tanaka**, Kawasaki, Japan

[73] Assignee: **Fujitsu Limited**, Kanagawa, Japan

[21] Appl. No.: **189,407**

[22] Filed: **Jan. 31, 1994**

[30] **Foreign Application Priority Data**

May 19, 1993 [JP] Japan 5-117189

[51] **Int. Cl.**[6] **H04J 3/02**; H04L 12/64

[52] **U.S. Cl.** **370/58.2**; 370/60.1; 370/79; 370/94.2; 370/112

[58] **Field of Search** 370/58.2, 58.3, 370/60, 79, 94.1, 112, 60.1, 94.2

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,999,835 3/1991 Lagoutte 370/94.1
5,339,318 8/1994 Tanaka et al. ..... 370/58.2 X

Primary Examiner—Douglas W. Olms
Assistant Examiner—Russell W. Blum

[57] **ABSTRACT**

A cell multiplexing apparatus includes a transmitting section in which information fields of a plurality of ATM cells intended for transmission along the same path are multiplexed and stored into an information field of one multiplexed cell. A representative VPI, globally representing the VPIs of the plurality of ATM cells intended for transmission along the same path, is assigned as the VPI of the multiplexed cell for transmission. A receiving section detects the representative VPI from received cells and the plurality of ATM cells having individual VPIs and transmitted along the same path are reconstructed from the multiplexed cell having the representative VPI. The VPI area of the ATM header of the multiplexed cell is divided into two segments. The representative VPI designating the path for the multiplexed cell is carried in one segment and VPI information of the plurality of ATM cells intended for transmission along the same path is carried in the other segment.

18 Claims, 25 Drawing Sheets

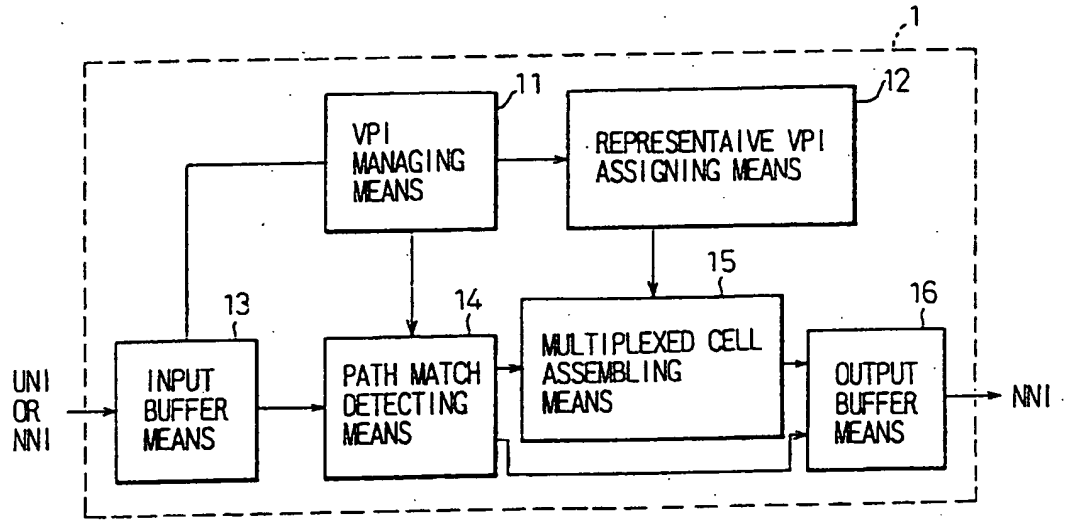


Fig.1

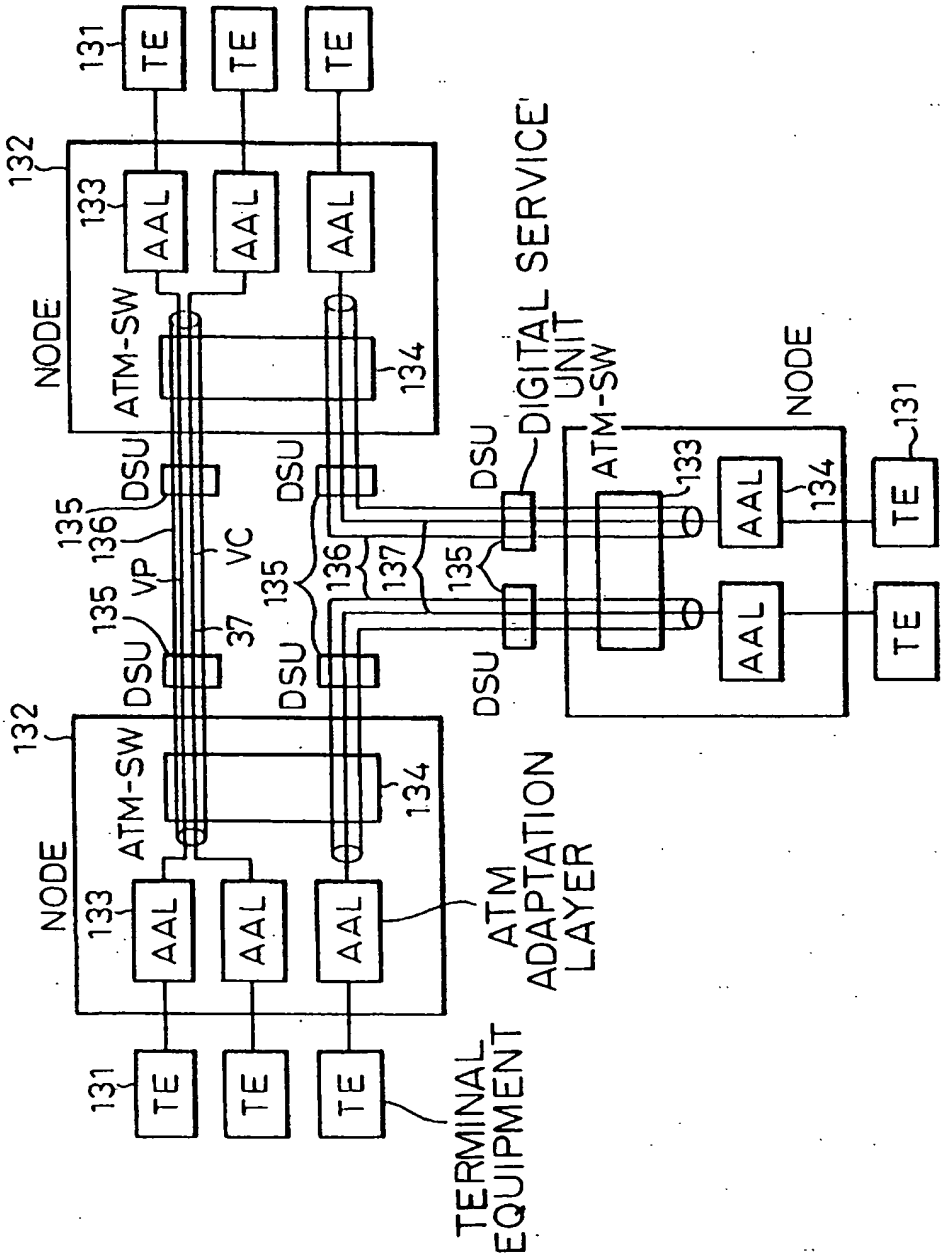

131
TE
132
133
AAL
NODE
ATM-SW
134
135
136
VP
VC
37
DSU
DIGITAL SERVICE UNIT
137
ATM ADAPTATION LAYER
TERMINAL EQUIPMENT

Fig.2

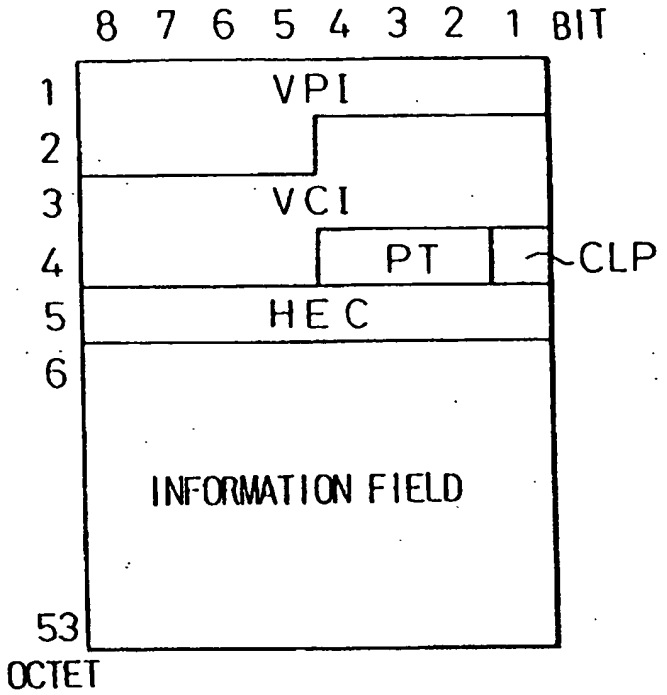

8 7 6 5 4 3 2 1 BIT
1
2
3
4
5
6
53
OCTET
VPI
VCI
PT
CLP
HEC
INFORMATION FIELD

Fig.3

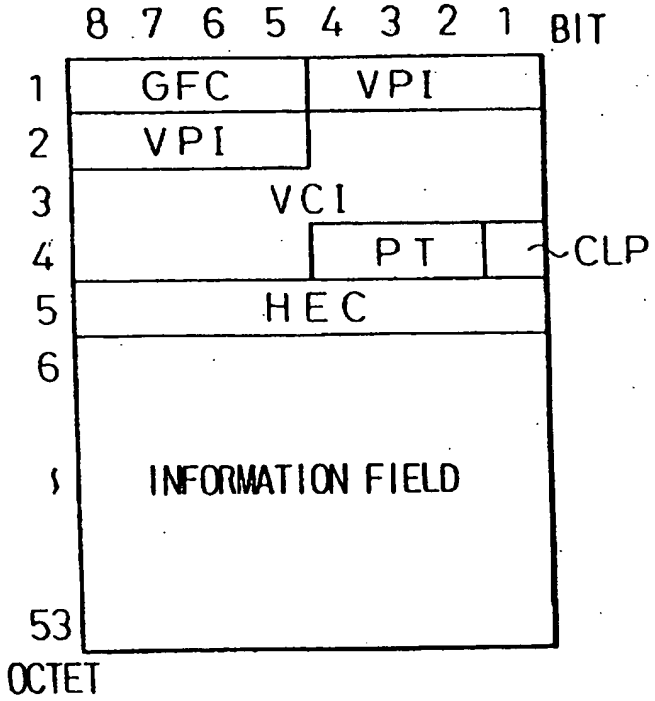

8 7 6 5 4 3 2 1 BIT
1
2
3
4
5
6
53
OCTET
GFC
VPI
VPI
VCI
PT
CLP
HEC
INFORMATION FIELD

Fig.4

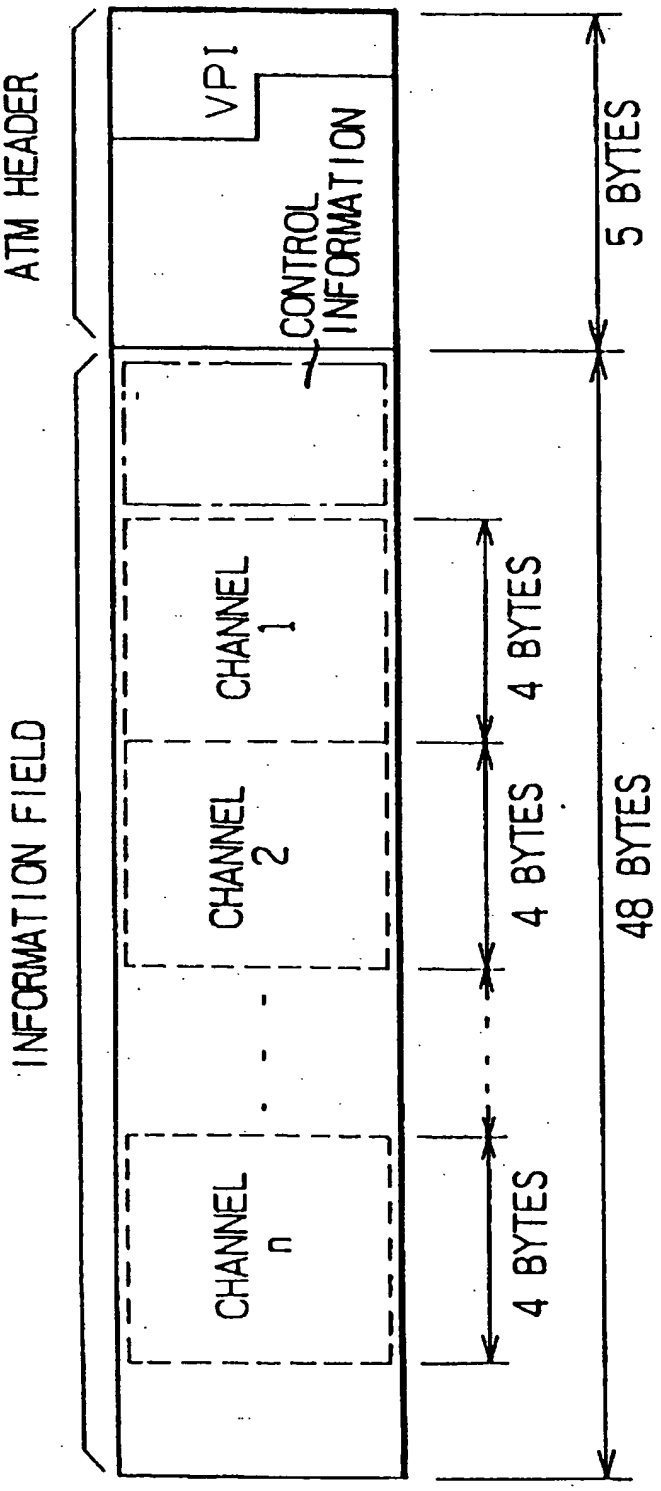

ATM HEADER
VPI
CONTROL INFORMATION
5 BYTES
INFORMATION FIELD
CHANNEL 1
CHANNEL 2
CHANNEL n
4 BYTES
4 BYTES
4 BYTES
48 BYTES

Fig.5

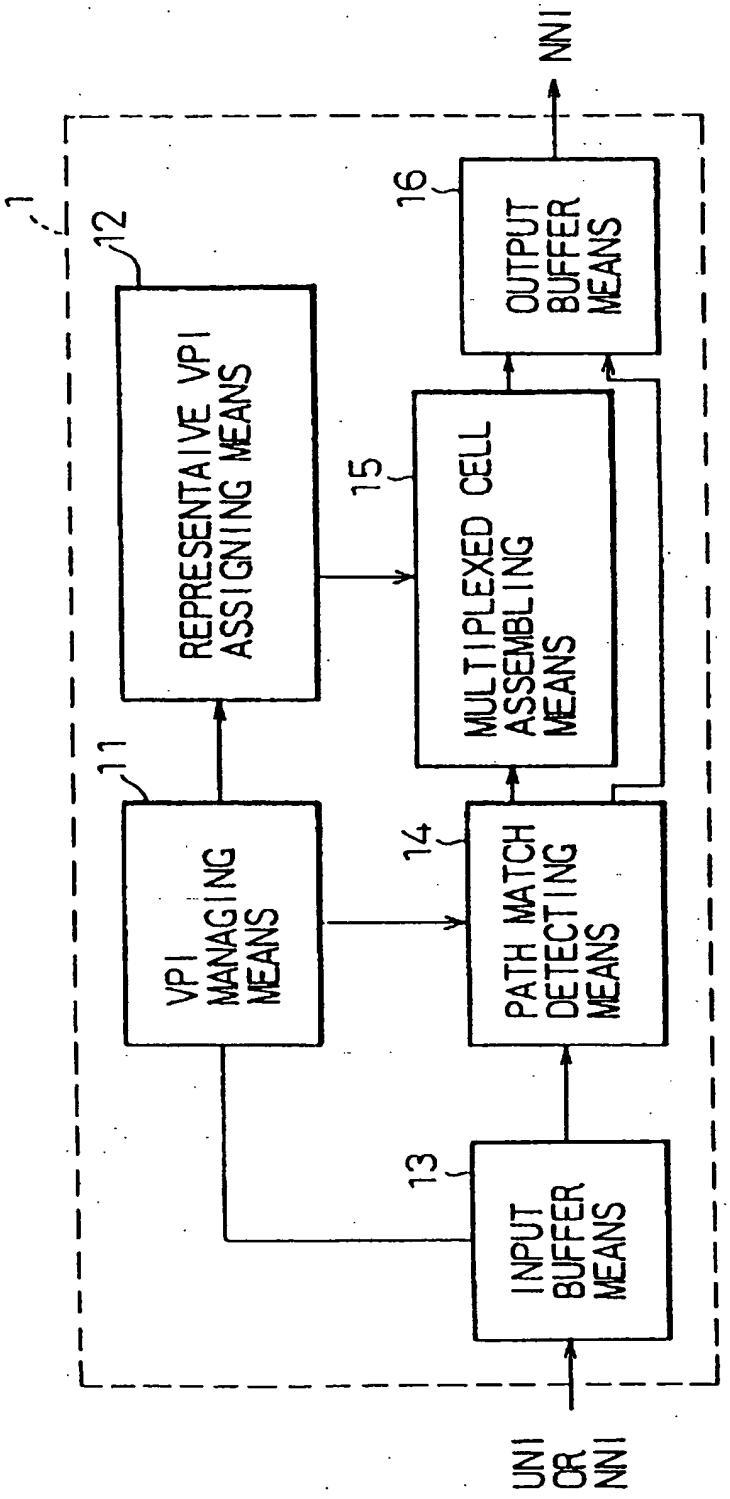

1
11
VPI MANAGING MEANS
12
REPRESENTAIVE VPI ASSIGNING MEANS
13
INPUT BUFFER MEANS
14
PATH MATCH DETECTING MEANS
15
MULTIPLEXED CELL ASSEMBLING MEANS
16
OUTPUT BUFFER MEANS
UNI OR NNI
NNI

Fig.6

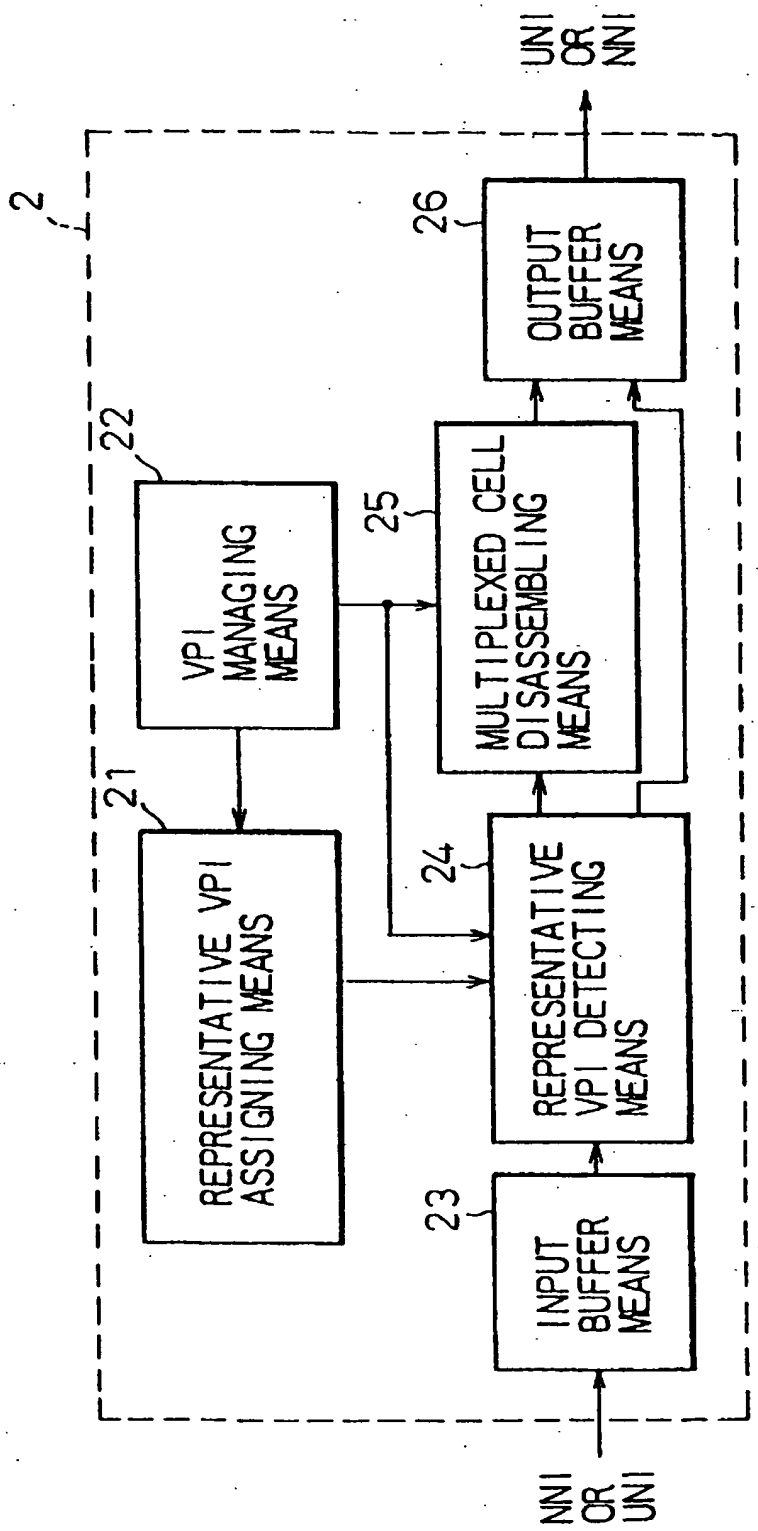

UNI OR NNI
2
26
OUTPUT BUFFER MEANS
22
VPI MANAGING MEANS
25
MULTIPLEXED CELL DISASSEMBLING MEANS
21
REPRESENTATIVE VPI ASSIGNING MEANS
24
REPRESENTATIVE VPI DETECTING MEANS
23
INPUT BUFFER MEANS
NNI OR UNI

Fig.7

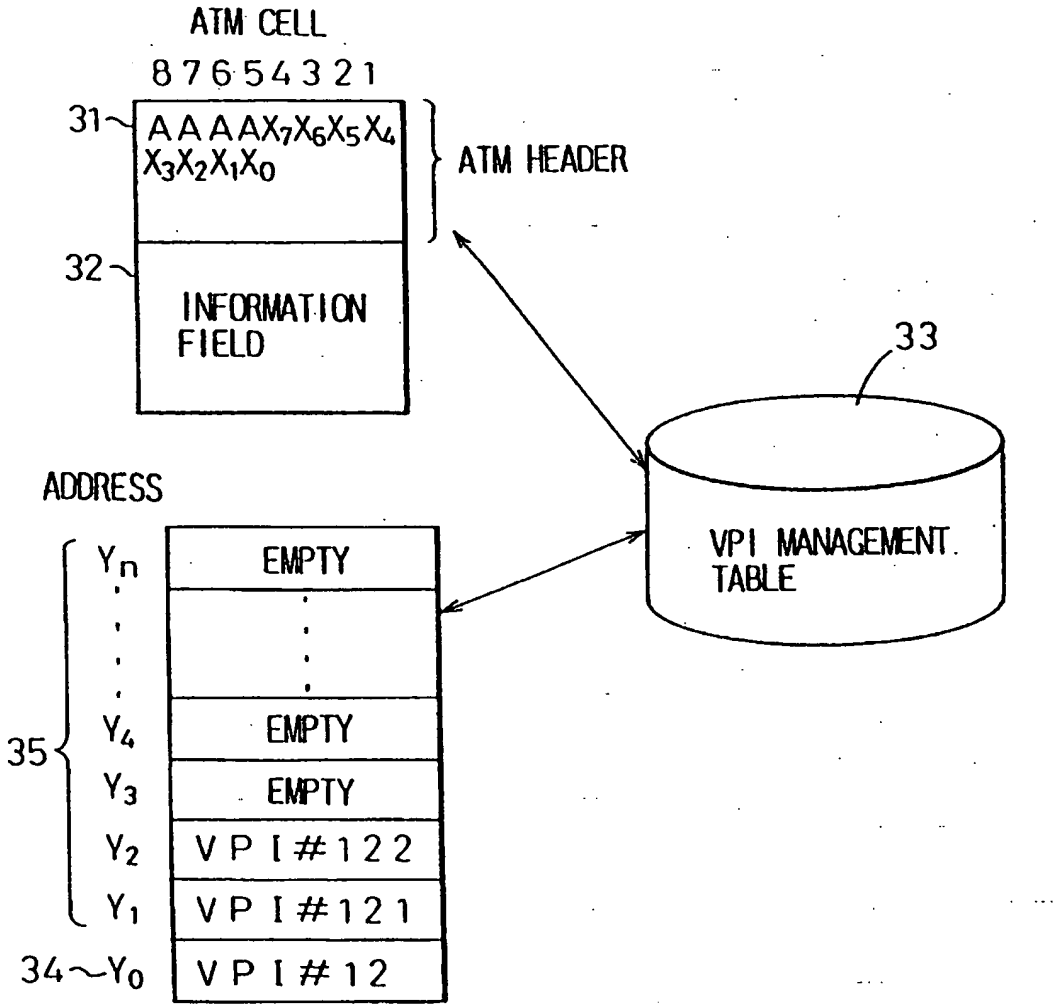

ATM CELL
8 7 6 5 4 3 2 1
31
AAAAX7X6X5X4
X3X2X1X0
ATM HEADER
32
INFORMATION FIELD
33
VPI MANAGEMENT TABLE
ADDRESS
Yn
EMPTY
Y4
EMPTY
Y3
EMPTY
Y2
VPI#122
Y1
VPI#121
34
Y0
VPI#12
35

Fig.8

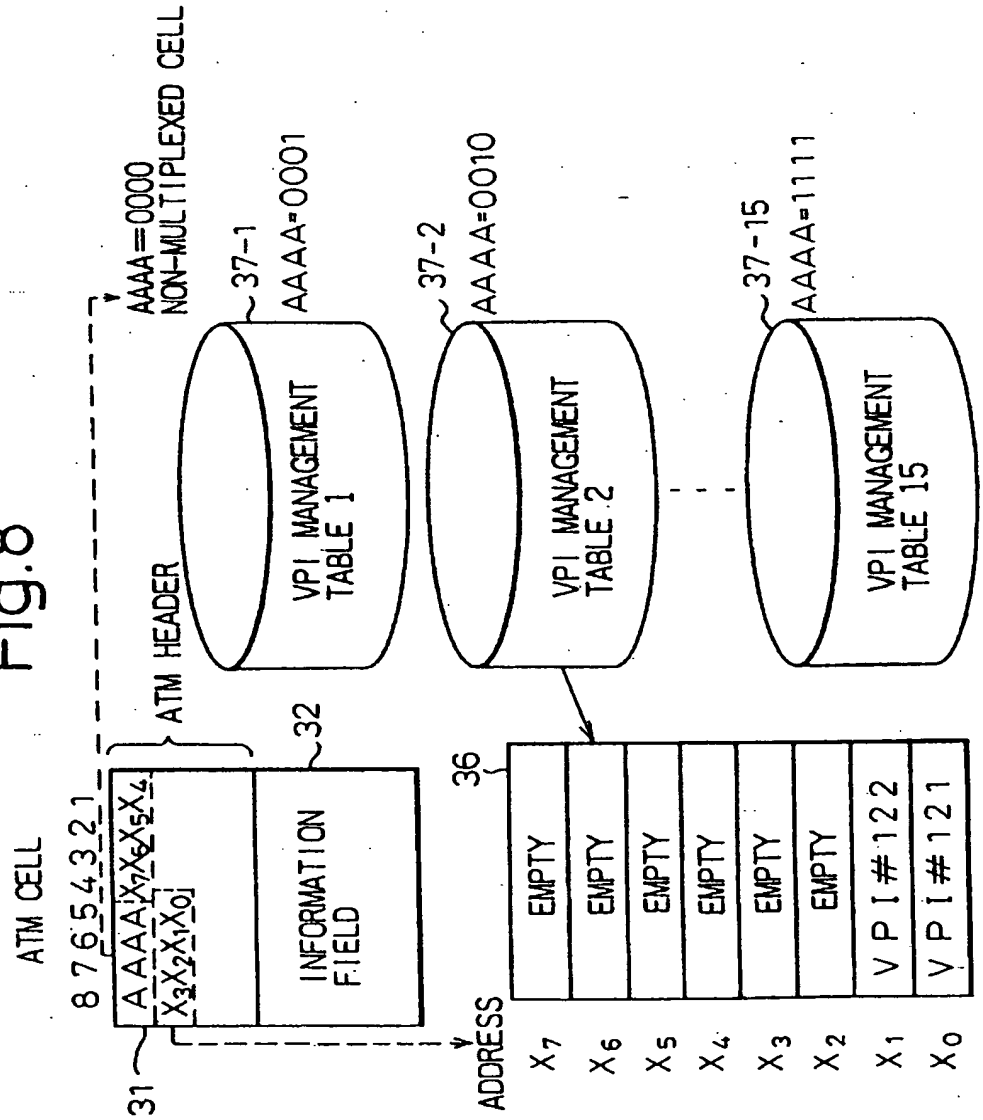

ATM CELL
8 7 6 5 4 3 2 1
A A A A X7 X6 X5 X4
X3 X2 X1 X0
ATM HEADER
INFORMATION FIELD
31
32
AAAA=0000
NON-MULTIPLEXED CELL
37-1
AAAA=0001
VPI MANAGEMENT TABLE 1
37-2
AAAA=0010
VPI MANAGEMENT TABLE 2
37-15
AAAA=1111
VPI MANAGEMENT TABLE 15
36
EMPTY
EMPTY
EMPTY
EMPTY
EMPTY
EMPTY
VPI#122
VPI#121
ADDRESS
X7 X6 X5 X4 X3 X2 X1 X0

Fig.9

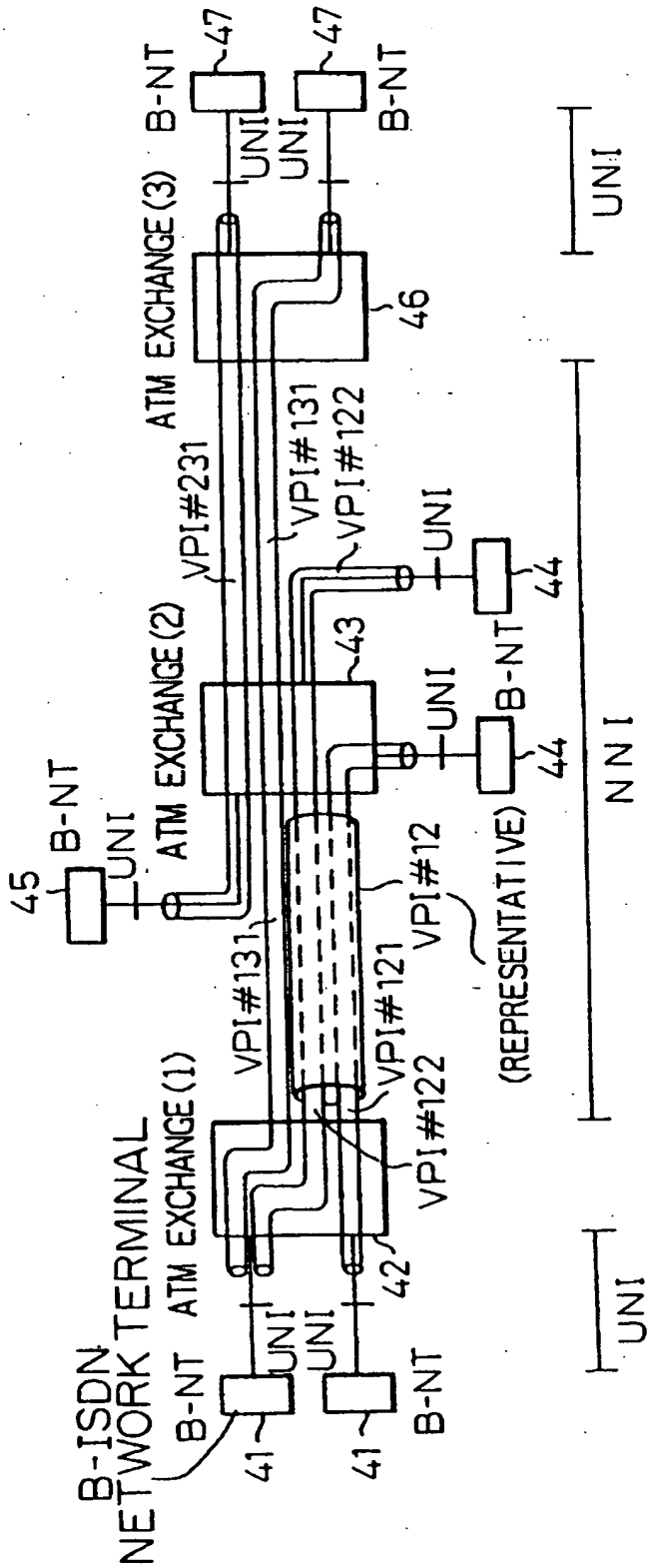

B-ISDN NETWORK TERMINAL
B-NT
UNI
ATM EXCHANGE (1)
ATM EXCHANGE (2)
ATM EXCHANGE (3)
41
42
43
44
45
46
47
VPI#131
VPI#121
VPI#122
VPI#12
VPI#231
(REPRESENTATIVE)
NNI

Fig.10

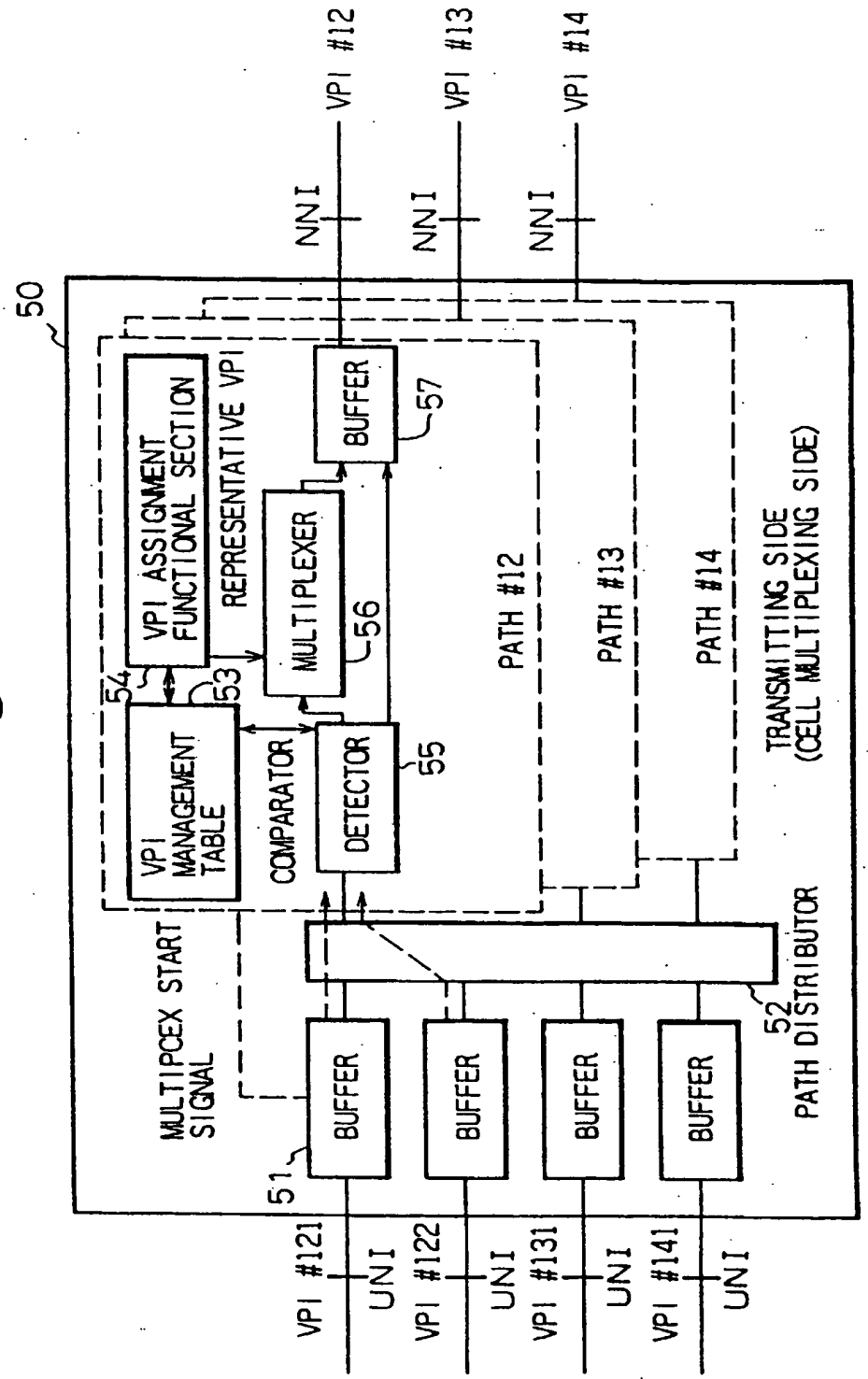

50
NNI
VPI #12
NNI
VPI #13
NNI
VPI #14
VPI ASSIGNMENT FUNCTIONAL SECTION
REPRESENTATIVE VPI
BUFFER
57
MULTIPLEXER
56
PATH #12
PATH #13
PATH #14
TRANSMITTING SIDE (CELL MULTIPLEXING SIDE)
54
53
VPI MANAGEMENT TABLE
COMPARATOR
DETECTOR
55
MULTIPCEX START SIGNAL
PATH DISTRIBUTOR
52
BUFFER
BUFFER
BUFFER
BUFFER
51
VPI #121
UNI
VPI #122
UNI
VPI #131
UNI
VPI #141
UNI

Fig.11

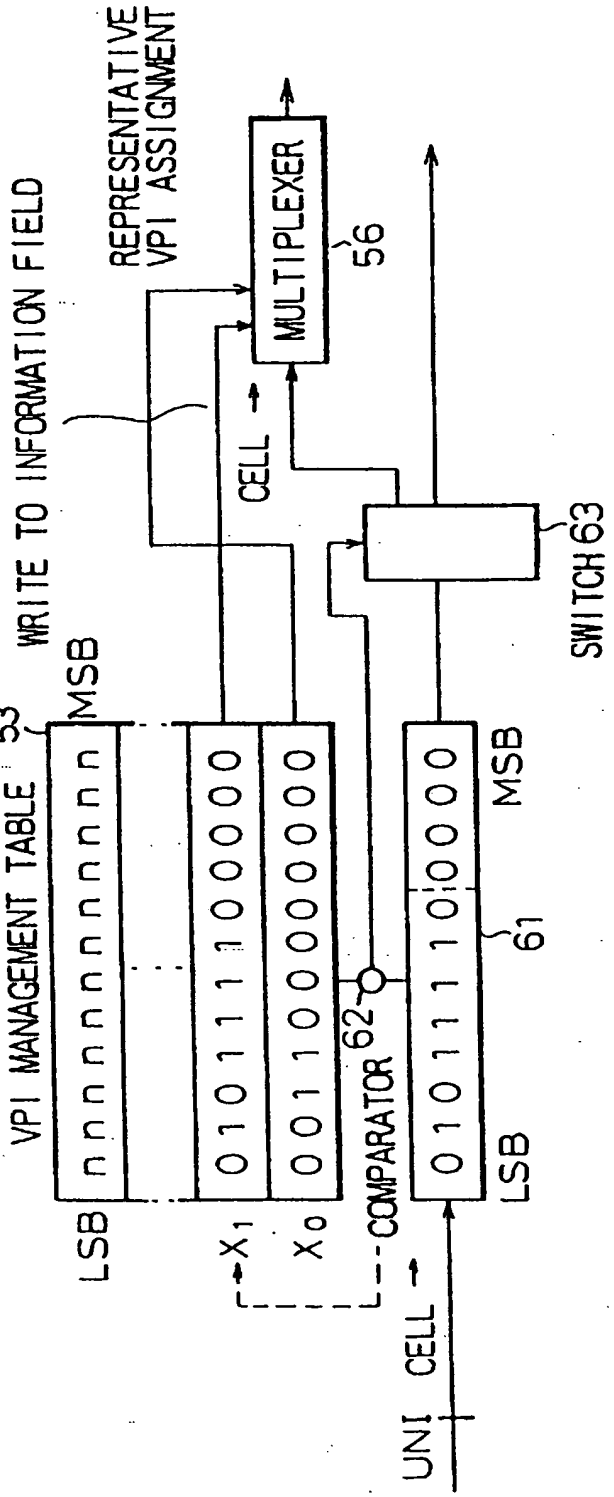

REPRESENTATIVE VPI ASSIGNMENT
MULTIPLEXER
56
WRITE TO INFORMATION FIELD
CELL
SWITCH 63
VPI MANAGEMENT TABLE
53
MSB
LSB
n n n n n n n n n n n n
0 1 0 1 1 1 1 0 0 0 0 0
0 0 1 1 0 0 0 0 0 0 0 0
X1
X0
COMPARATOR
62
0 1 0 1 1 1 1 0 0 0 0 0
61
MSB
LSB
UNI CELL

Fig.12

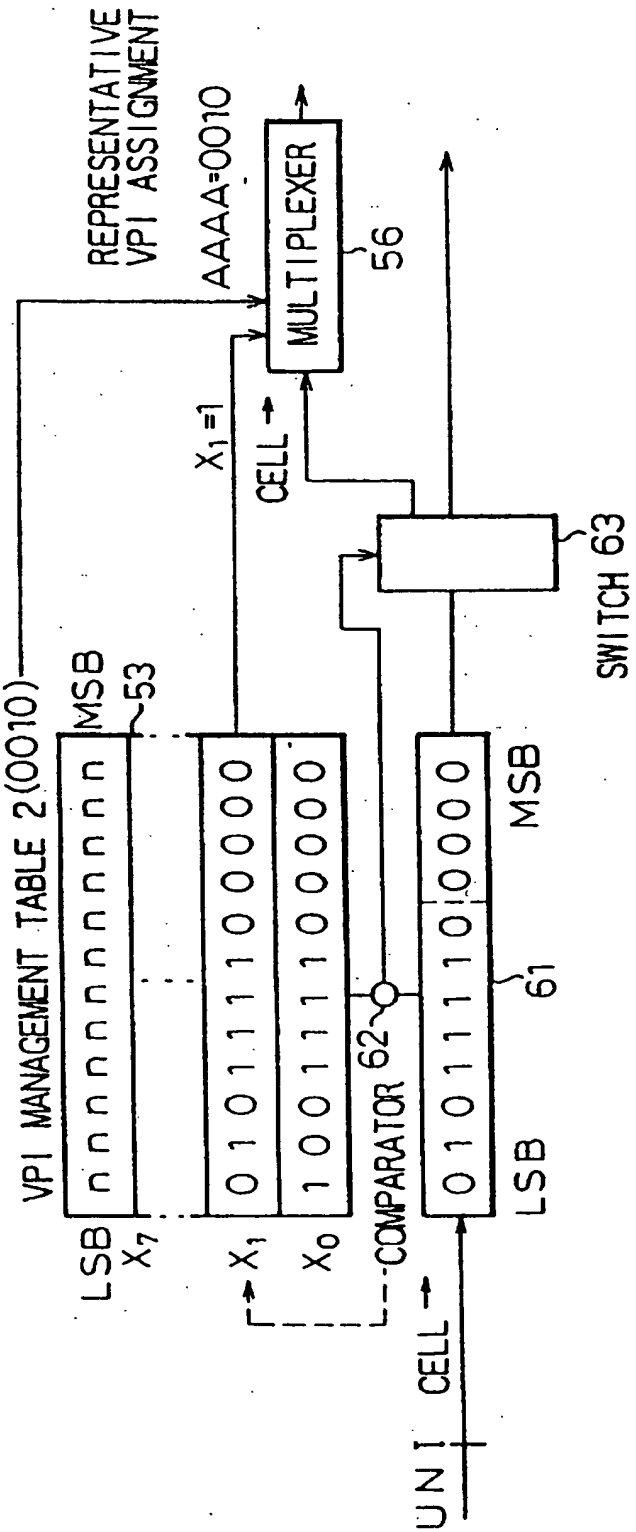

REPRESENTATIVE VPI ASSIGNMENT
AAAA=0010
MULTIPLEXER
56
X_1=1
CELL
SWITCH 63
VPI MANAGEMENT TABLE 2(0010)
MSB
53
nnnnnnnnnnnnnnnn
0101111100000000
1001111100000000
0101111101000000
MSB
61
LSB
X_7
X_1
X_0
COMPARATOR 62
LSB
UNI CELL

Fig.13

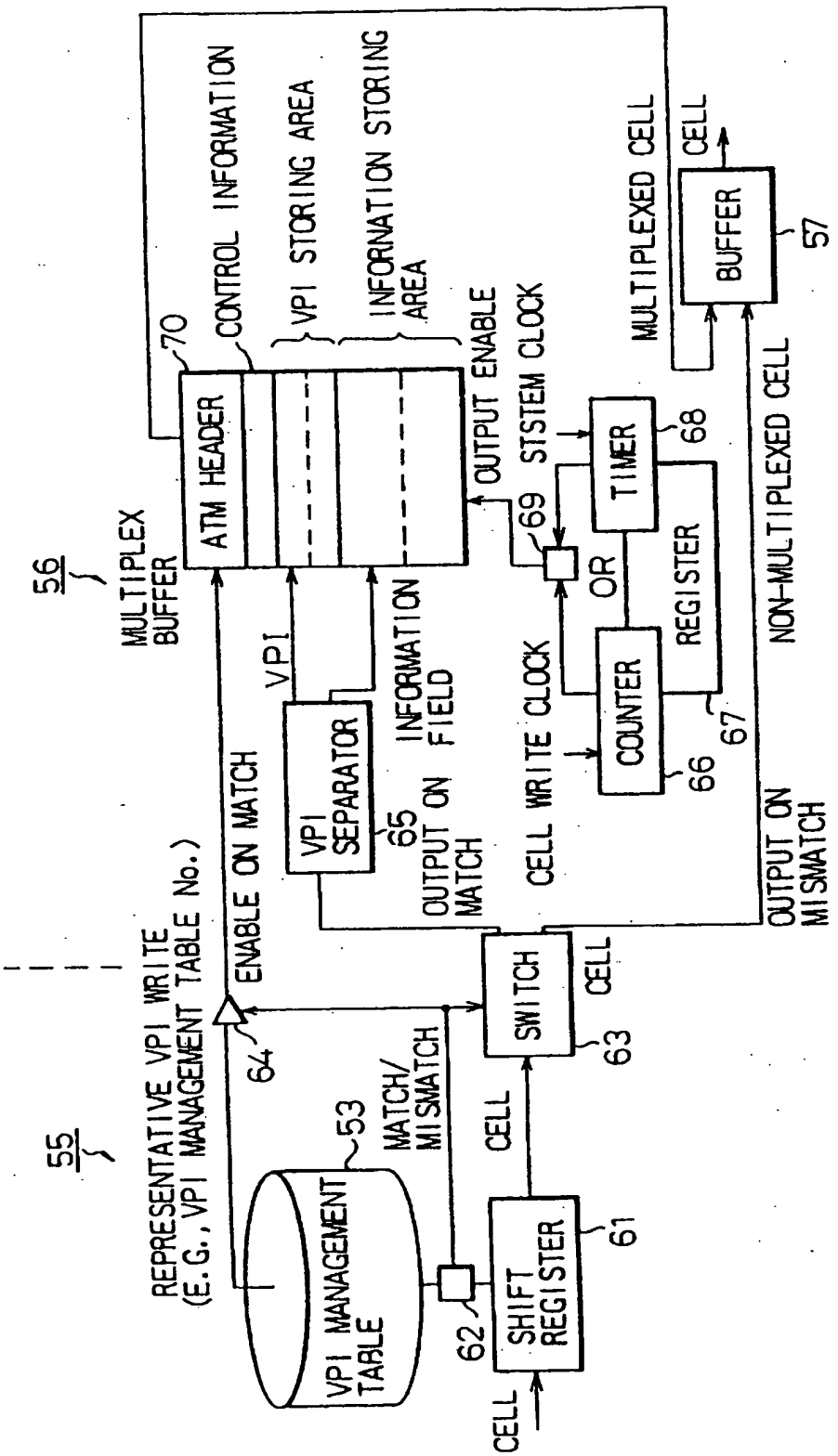

55
56
REPRESENTATIVE VPI WRITE (E.G., VPI MANAGEMENT TABLE No.)
MULTIPLEX BUFFER
ATM HEADER
CONTROL INFORMATION
VPI STORING AREA
INFORMATION STORING AREA
70
ENABLE ON MATCH
64
VPI
VPI SEPARATOR
65
INFORMATION FIELD
OUTPUT ON MATCH
OUTPUT ENABLE
69
SYSTEM CLOCK
CELL WRITE CLOCK
OR
TIMER
68
COUNTER
66
REGISTER
67
MULTIPLEXED CELL
CELL
BUFFER
57
NON-MULTIPLEXED CELL
OUTPUT ON MISMATCH
SWITCH
63
CELL
MATCH/ MISMATCH
53
VPI MANAGEMENT TABLE
62
SHIFT REGISTER
61
CELL

Fig.14

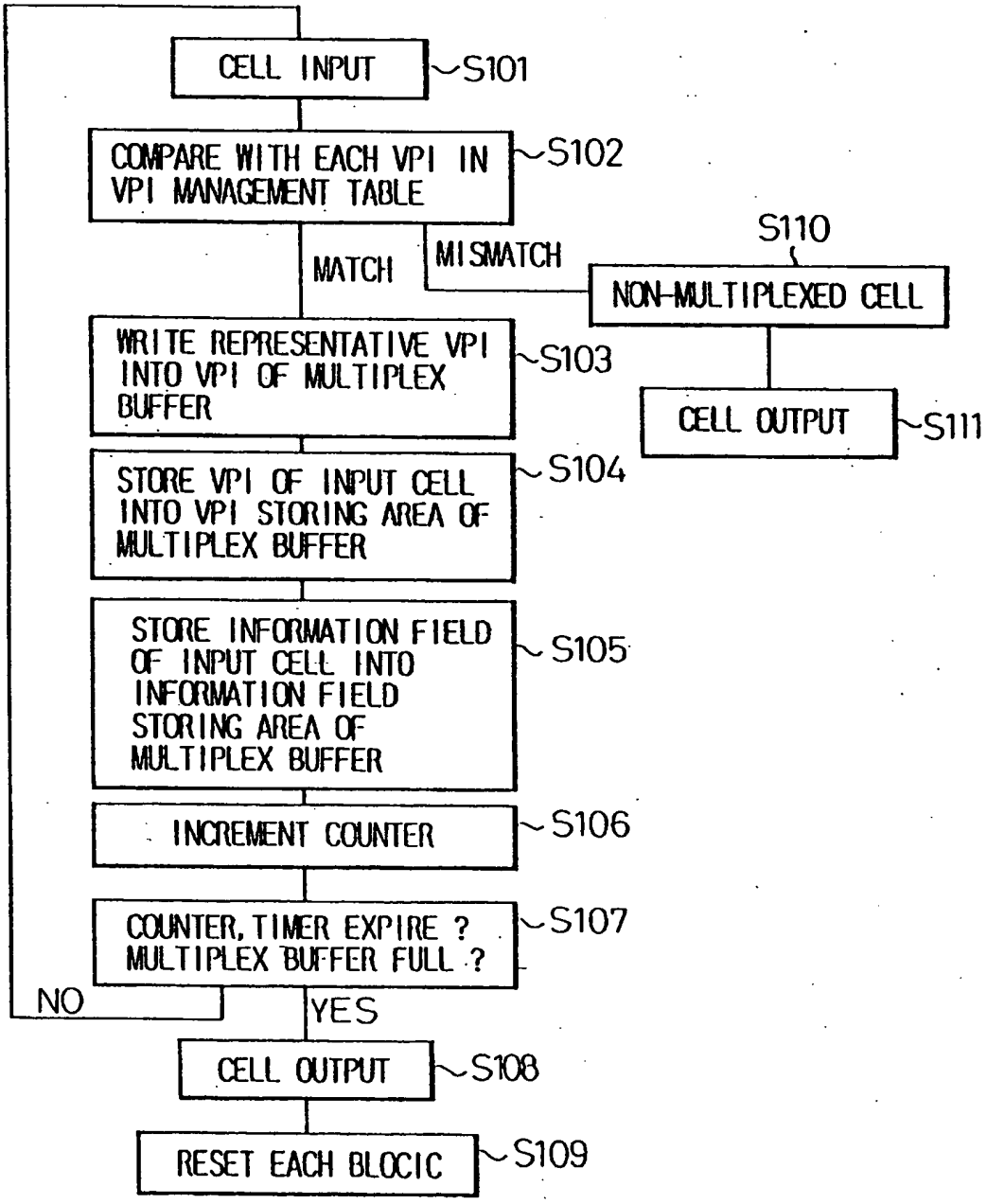

CELL INPUT
S101
COMPARE WITH EACH VPI IN VPI MANAGEMENT TABLE
S102
MATCH
MISMATCH
S110
NON-MULTIPLEXED CELL
CELL OUTPUT
S111
WRITE REPRESENTATIVE VPI INTO VPI OF MULTIPLEX BUFFER
S103
STORE VPI OF INPUT CELL INTO VPI STORING AREA OF MULTIPLEX BUFFER
S104
STORE INFORMATION FIELD OF INPUT CELL INTO INFORMATION FIELD STORING AREA OF MULTIPLEX BUFFER
S105
INCREMENT COUNTER
S106
COUNTER, TIMER EXPIRE ? MULTIPLEX BUFFER FULL ?
S107
NO
YES
CELL OUTPUT
S108
RESET EACH BLOCIC
S109

Fig.15

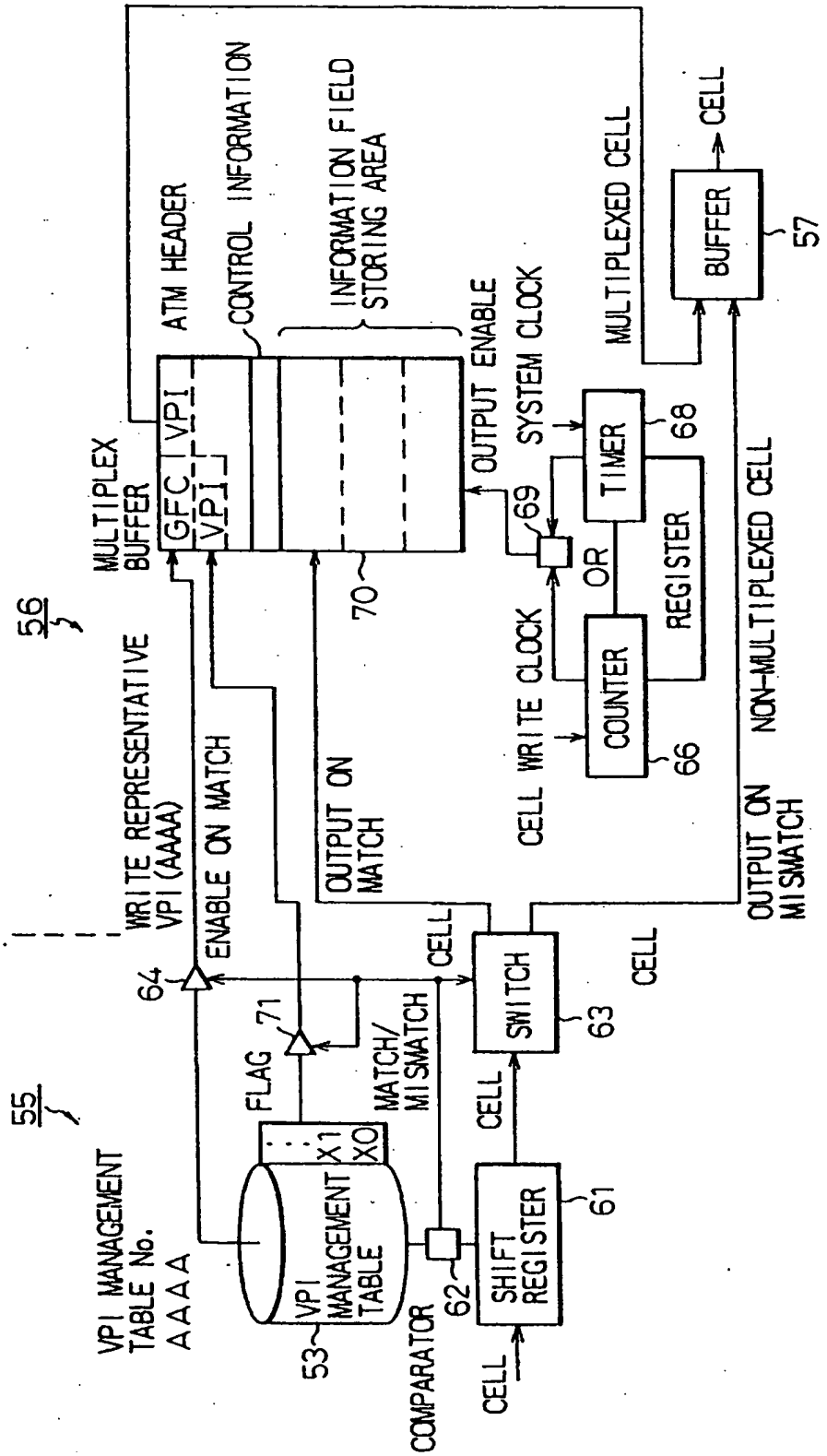

56
55
MULTIPLEX BUFFER
GFC
VPI
VPI
ATM HEADER
CONTROL INFORMATION
INFORMATION FIELD STORING AREA
OUTPUT ENABLE
70
69
SYSTEM CLOCK
TIMER
68
OR
REGISTER
COUNTER
66
CELL WRITE CLOCK
MULTIPLEXED CELL
BUFFER
CELL
57
WRITE REPRESENTATIVE VPI (AAAA)
64
ENABLE ON MATCH
OUTPUT ON MATCH
CELL
SWITCH
63
CELL
OUTPUT ON MISMATCH
NON-MULTIPLEXED CELL
71
FLAG
MATCH/ MISMATCH
X1
XO
VPI MANAGEMENT TABLE No. AAAA
VPI MANAGEMENT TABLE
53
COMPARATOR
62
SHIFT REGISTER
61
CELL

Fig.16

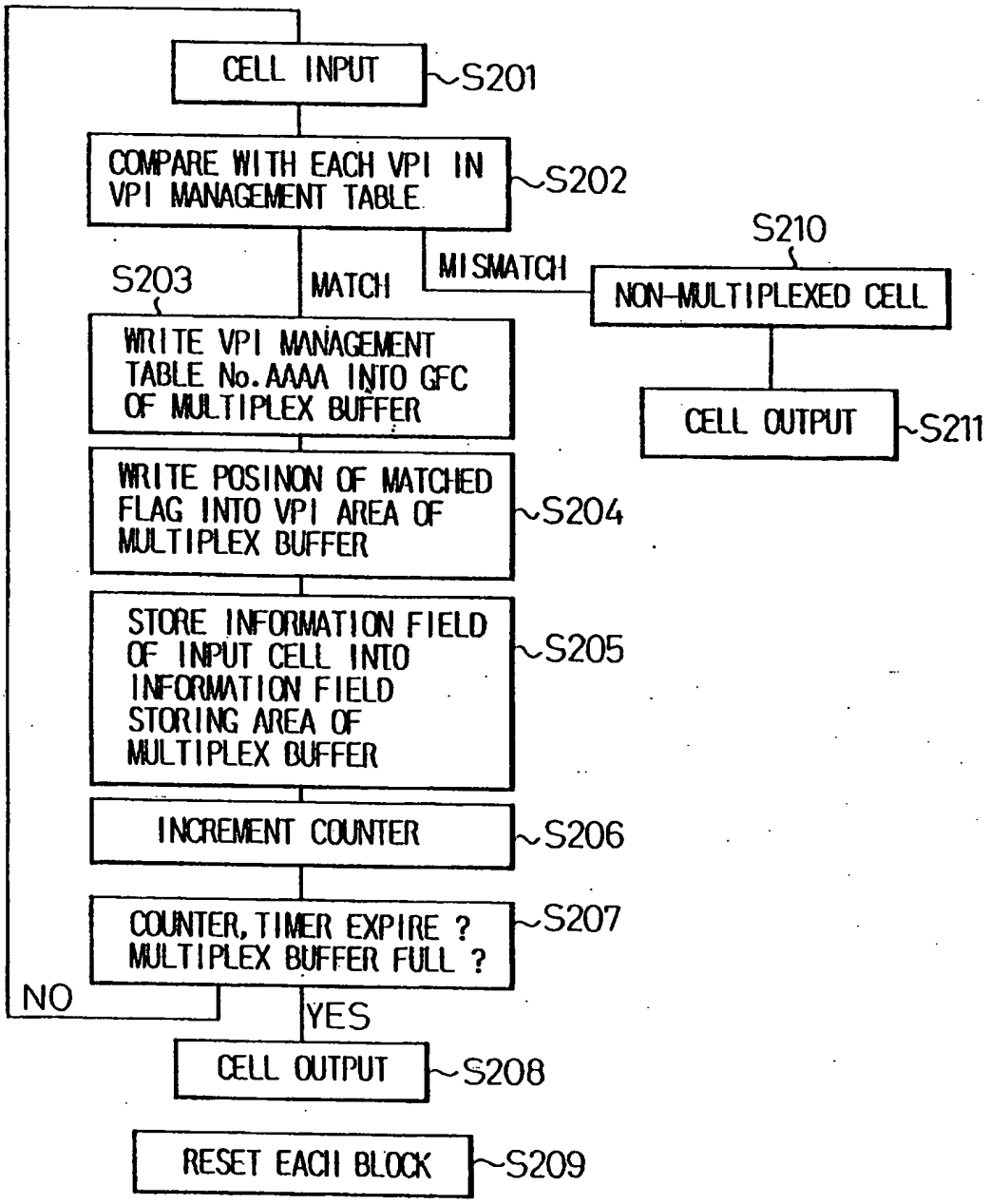

CELL INPUT
S201
COMPARE WITH EACH VPI IN VPI MANAGEMENT TABLE
S202
S210
MISMATCH
NON-MULTIPLEXED CELL
CELL OUTPUT
S211
S203
MATCH
WRITE VPI MANAGEMENT TABLE No. AAAA INTO GFC OF MULTIPLEX BUFFER
WRITE POSINON OF MATCHED FLAG INTO VPI AREA OF MULTIPLEX BUFFER
S204
STORE INFORMATION FIELD OF INPUT CELL INTO INFORMATION FIELD STORING AREA OF MULTIPLEX BUFFER
S205
INCREMENT COUNTER
S206
COUNTER, TIMER EXPIRE ? MULTIPLEX BUFFER FULL ?
S207
NO
YES
CELL OUTPUT
S208
RESET EACH BLOCK
S209

Fig.17

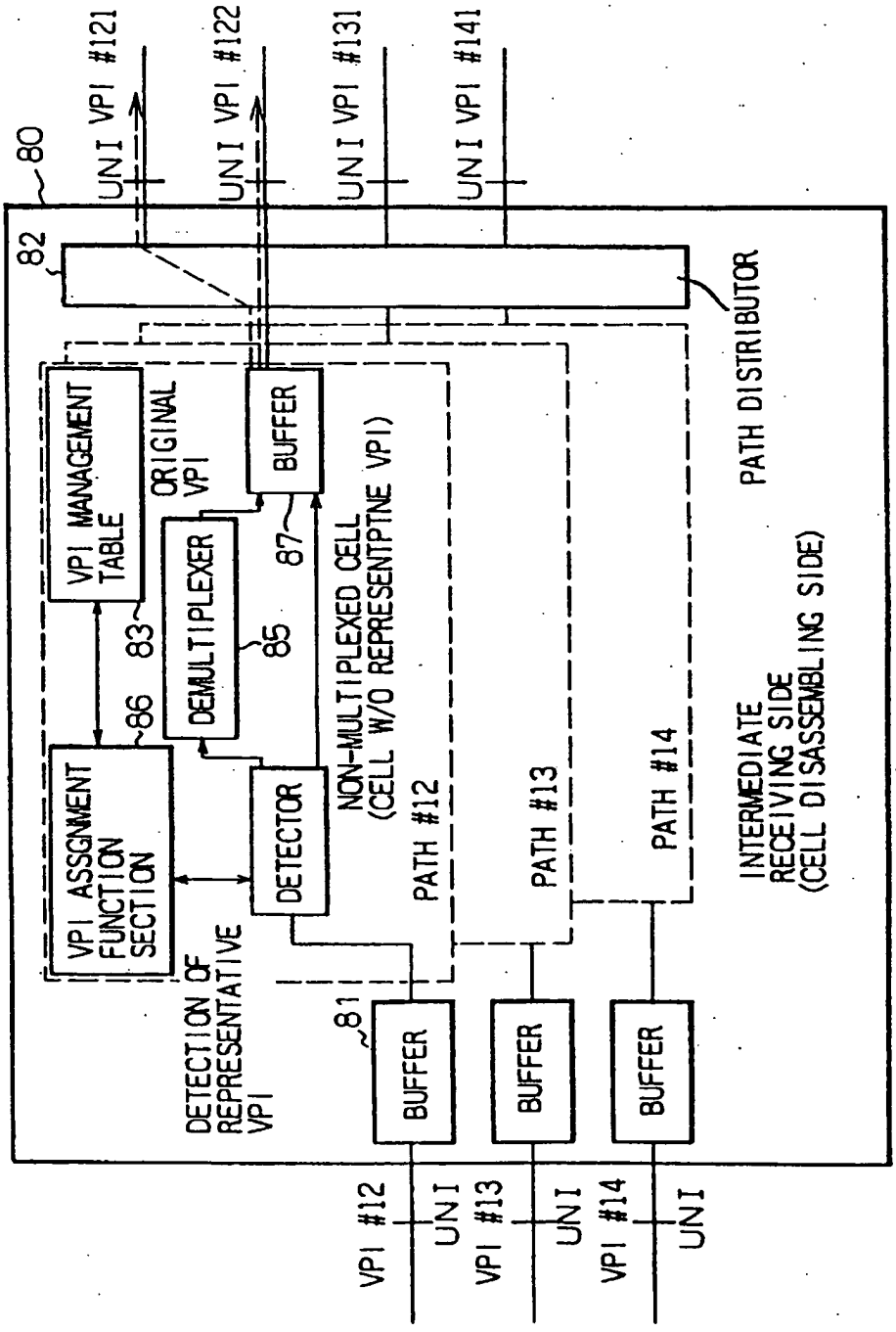

80
UNI VPI #121
UNI VPI #122
UNI VPI #131
UNI VPI #141
82
PATH DISTRIBUTOR
VPI MANAGEMENT TABLE
ORIGINAL VPI
BUFFER
DEMULTIPLEXER
87
85
83
86
NON-MULTIPLEXED CELL (CELL W/O REPRESENTPTINE VPI)
VPI ASSGNMENT FUNCTION SECTION
DETECTOR
PATH #12
PATH #13
PATH #14
INTERMEDIATE RECEIVING SIDE (CELL DISASSEMBLING SIDE)
DETECTION OF REPRESENTATIVE VPI
81
BUFFER
BUFFER
BUFFER
VPI #12
UNI
VPI #13
UNI
VPI #14
UNI

Fig.18

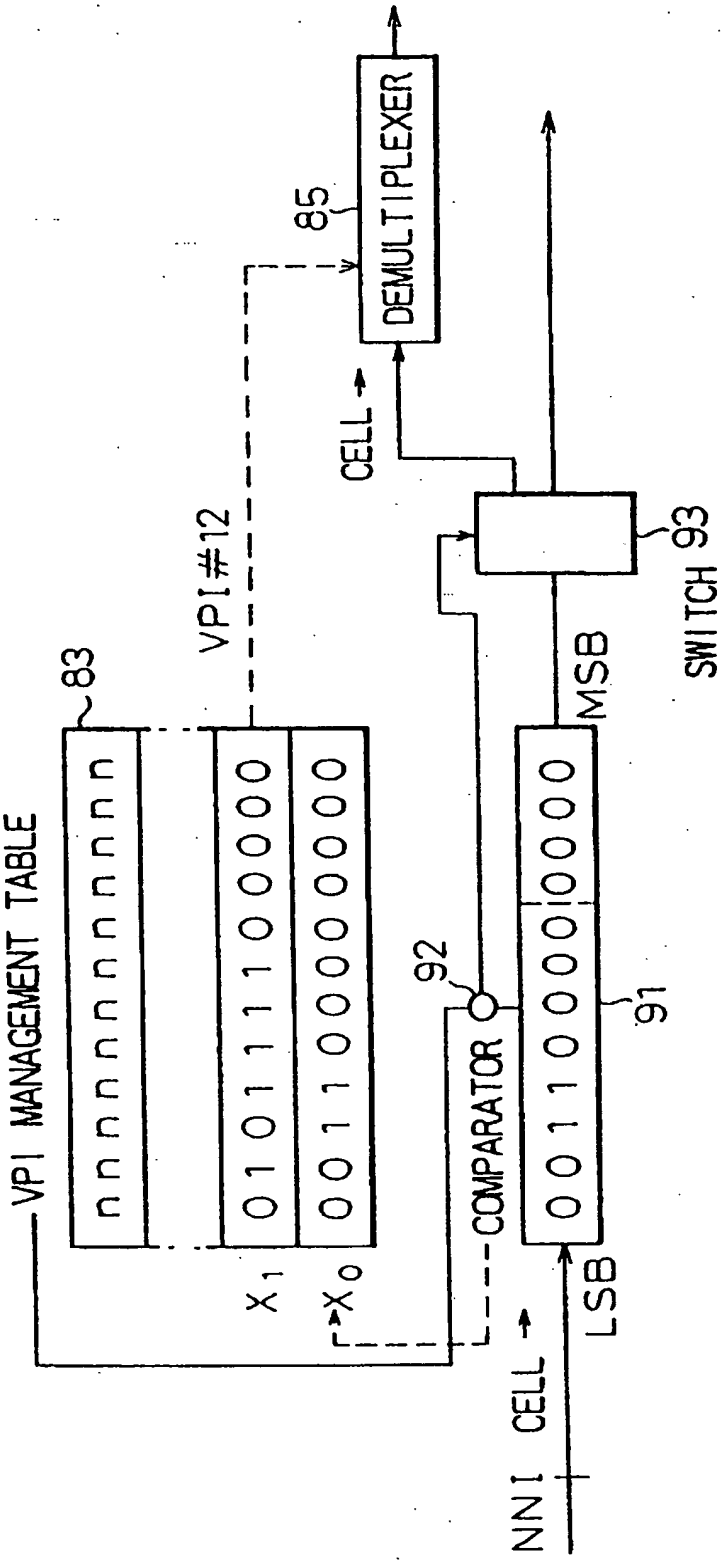

DEMULTIPLEXER
85
CELL
VPI #12
83
SWITCH 93
MSB
VPI MANAGEMENT TABLE
nnnnnnnnnn
0101111000000
0011000000000
92
COMPARATOR
0011000010000
91
X1
X0
LSB
NNI CELL

Fig.19

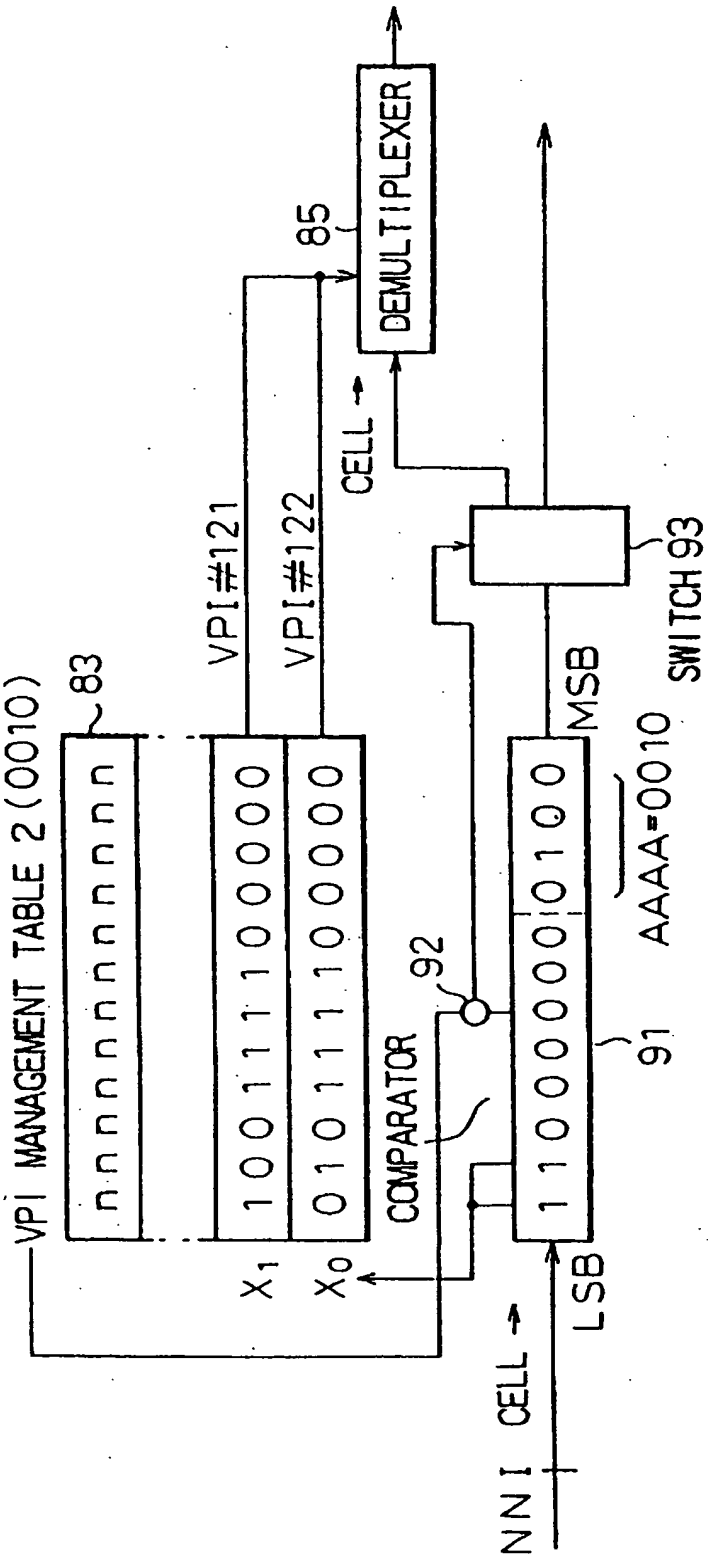

DEMULTIPLEXER
85
CELL
VPI #121
VPI #122
SWITCH 93
MSB
AAAA=0010
VPI MANAGEMENT TABLE 2 (0010)
83
nnnnnnnnnnnn
100111100000
010111100000
110000001100
91
92
COMPARATOR
X1
X0
LSB
NNI CELL

Fig.20

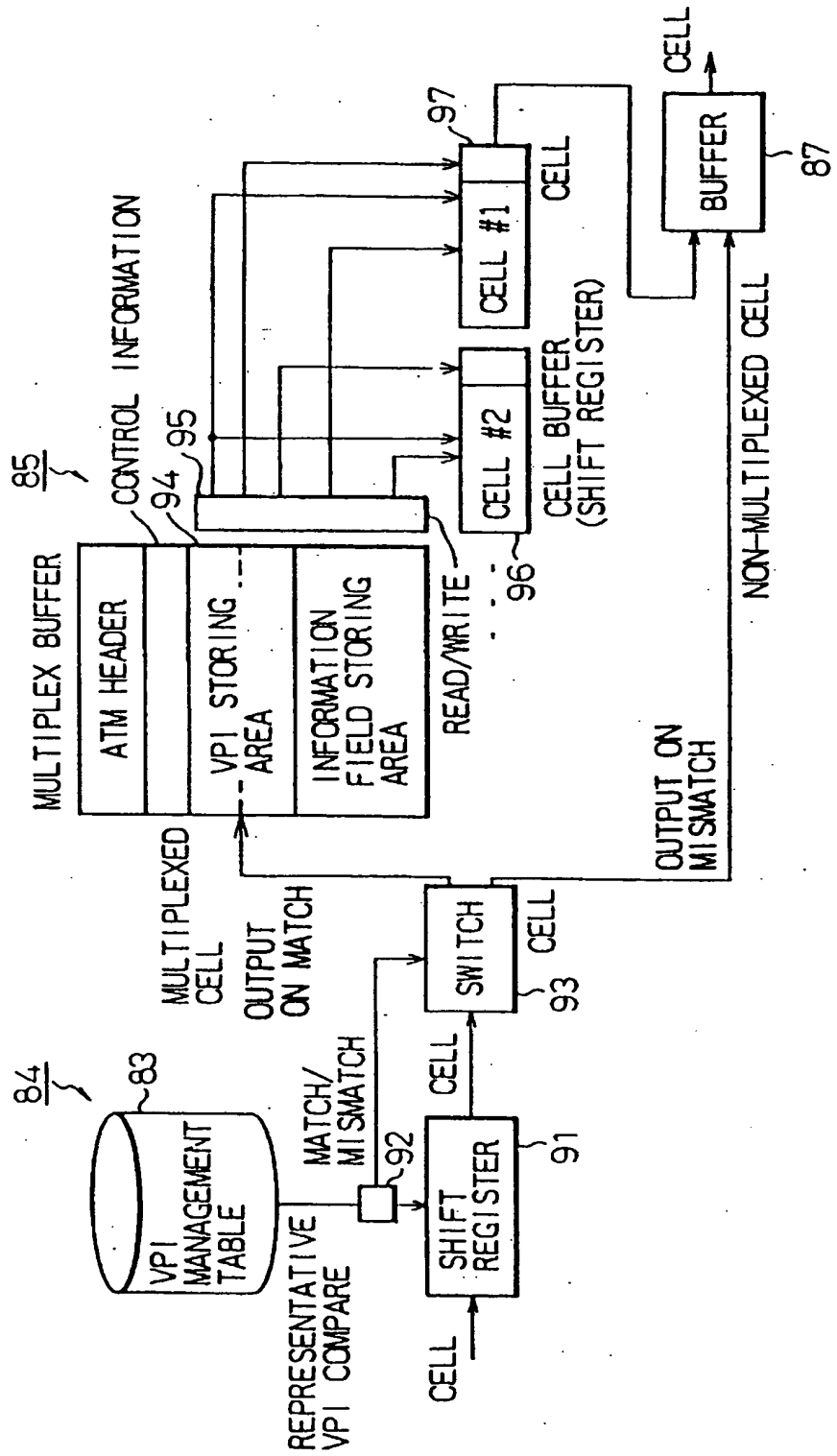

84
83
VPI MANAGEMENT TABLE
REPRESENTATIVE VPI COMPARE
MATCH/ MISMATCH
92
SHIFT REGISTER
91
CELL
CELL
SWITCH
93
CELL
MULTIPLEX BUFFER
ATM HEADER
VPI STORING AREA
INFORMATION FIELD STORING AREA
85
CONTROL INFORMATION
94
95
READ/WRITE
96
CELL #1
CELL #2
97
CELL BUFFER (SHIFT REGISTER)
CELL
BUFFER
87
CELL
NON-MULTIPLEXED CELL
OUTPUT ON MISMATCH
MULTIPLEXED CELL
OUTPUT ON MATCH

Fig. 21

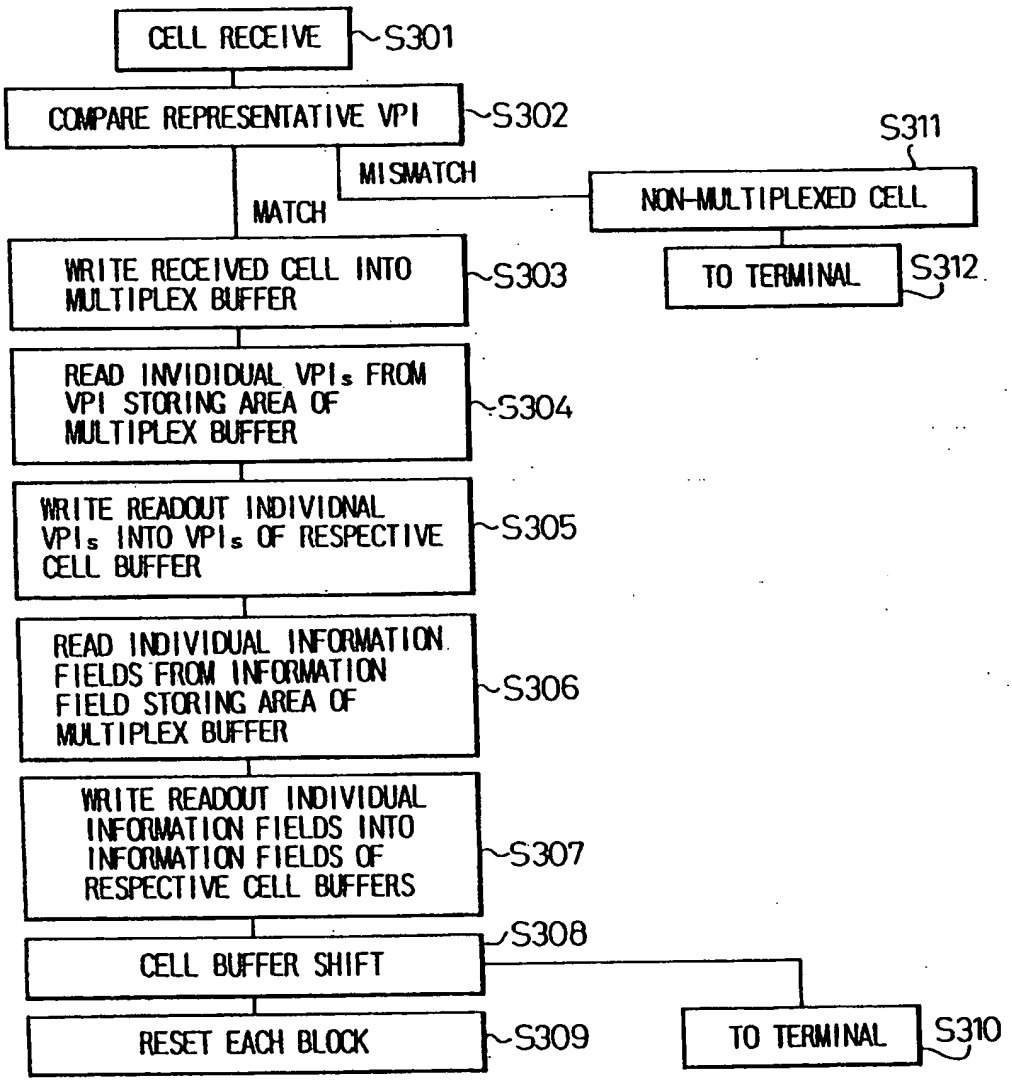

CELL RECEIVE
S301
COMPARE REPRESENTATIVE VPI
S302
MISMATCH
MATCH
S311
NON-MULTIPLEXED CELL
TO TERMINAL
S312
WRITE RECEIVED CELL INTO MULTIPLEX BUFFER
S303
READ INVIDIDUAL VPIs FROM VPI STORING AREA OF MULTIPLEX BUFFER
S304
WRITE READOUT INDIVIDNAL VPIs INTO VPIs OF RESPECTIVE CELL BUFFER
S305
READ INDIVIDUAL INFORMATION FIELDS FROM INFORMATION FIELD STORING AREA OF MULTIPLEX BUFFER
S306
WRITE READOUT INDIVIDUAL INFORMATION FIELDS INTO INFORMATION FIELDS OF RESPECTIVE CELL BUFFERS
S307
CELL BUFFER SHIFT
S308
RESET EACH BLOCK
S309
TO TERMINAL
S310

Fig.22

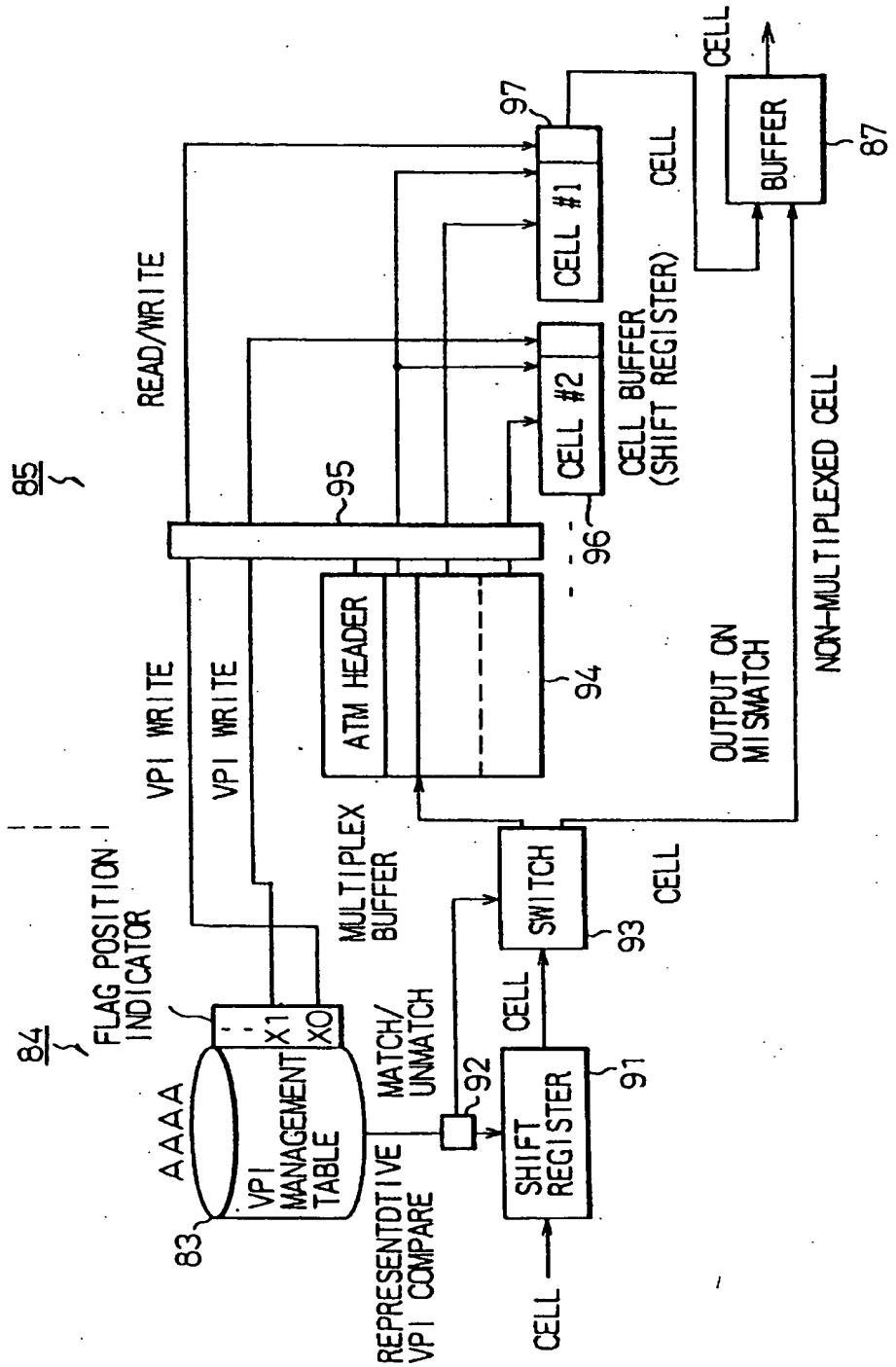

READ/WRITE
85
95
97
CELL #1
CELL #2
96
CELL BUFFER
(SHIFT REGISTER)
CELL
BUFFER
87
NON-MULTIPLEXED CELL
OUTPUT ON
MISMATCH
ATM HEADER
94
VPI WRITE
VPI WRITE
MULTIPLEX
BUFFER
SWITCH
93
CELL
84
FLAG POSITION
INDICATOR
X1
XO
AAAA
VPI
MANAGEMENT
TABLE
83
MATCH/
UNMATCH
92
CELL
SHIFT
REGISTER
91
REPRESENTDTIVE
VPI COMPARE
CELL

Fig. 23

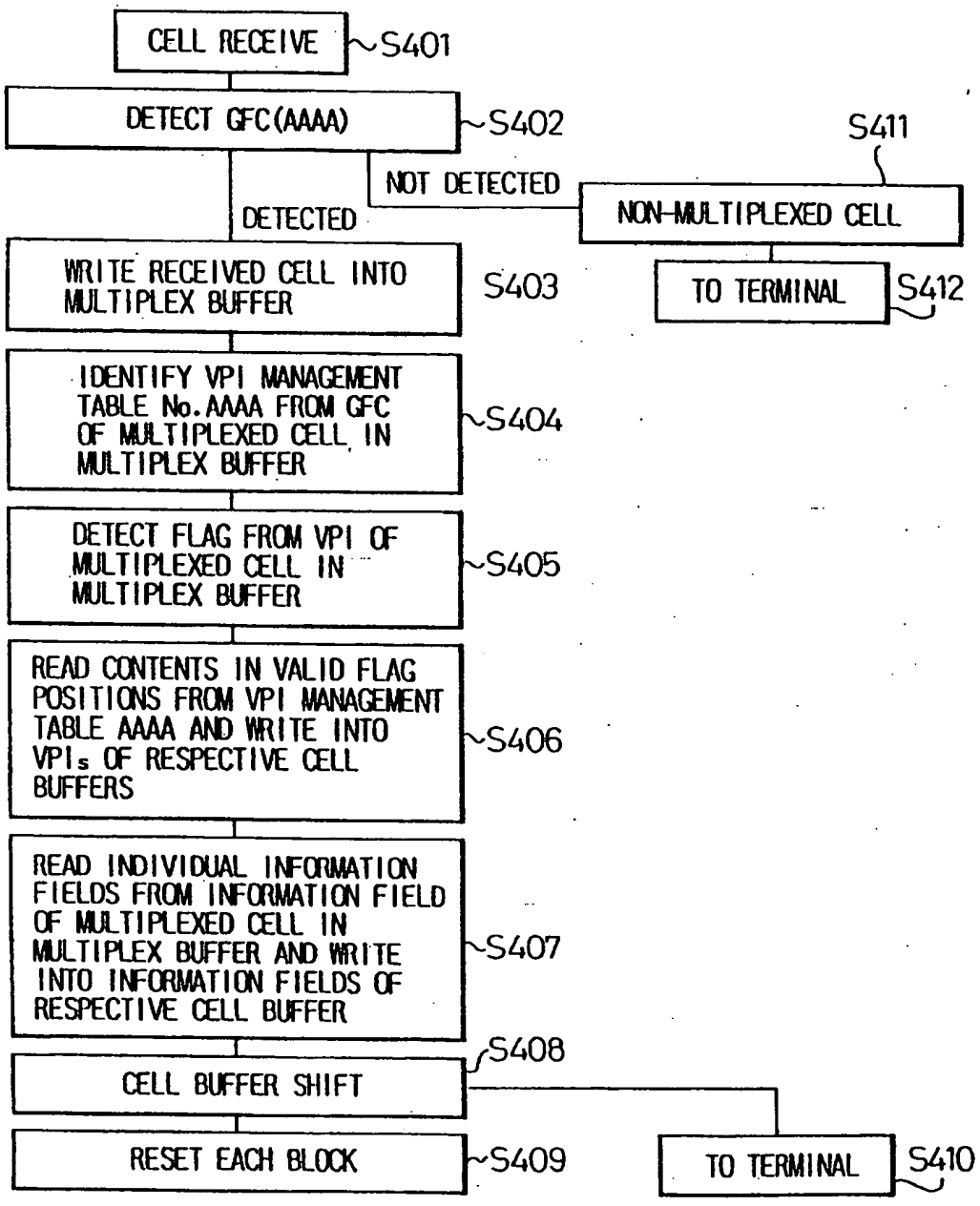

CELL RECEIVE
S401
DETECT GFC(AAAA)
S402
NOT DETECTED
DETECTED
S411
NON-MULTIPLEXED CELL
TO TERMINAL
S412
WRITE RECEIVED CELL INTO MULTIPLEX BUFFER
S403
IDENTIFY VPI MANAGEMENT TABLE No. AAAA FROM GFC OF MULTIPLEXED CELL IN MULTIPLEX BUFFER
S404
DETECT FLAG FROM VPI OF MULTIPLEXED CELL IN MULTIPLEX BUFFER
S405
READ CONTENTS IN VALID FLAG POSITIONS FROM VPI MANAGEMENT TABLE AAAA AND WRITE INTO VPIs OF RESPECTIVE CELL BUFFERS
S406
READ INDIVIDUAL INFORMATION FIELDS FROM INFORMATION FIELD OF MULTIPLEXED CELL IN MULTIPLEX BUFFER AND WRITE INTO INFORMATION FIELDS OF RESPECTIVE CELL BUFFER
S407
S408
CELL BUFFER SHIFT
RESET EACH BLOCK
S409
TO TERMINAL
S410

Fig.24

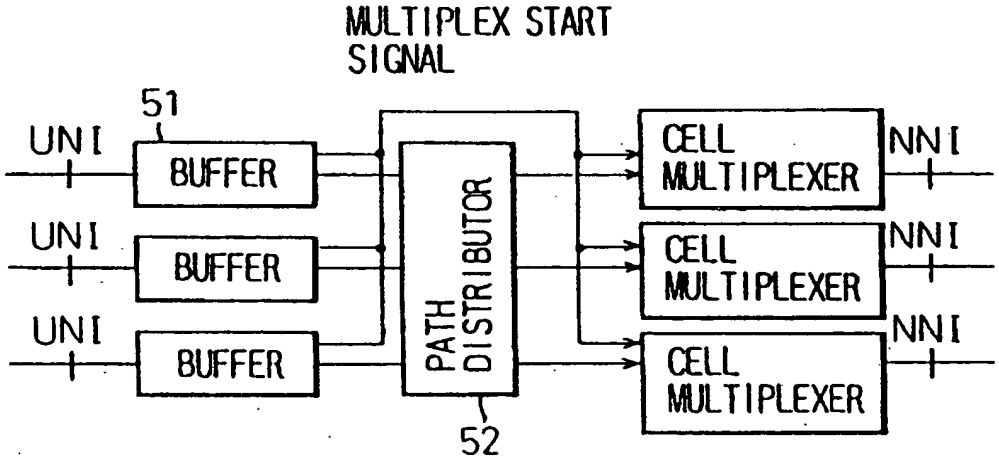

MULTIPLEX START SIGNAL
51
UNI
UNI
UNI
BUFFER
BUFFER
BUFFER
PATH DISTRIBUTOR
52
CELL MULTIPLEXER
CELL MULTIPLEXER
CELL MULTIPLEXER
NNI
NNI
NNI

Fig. 25

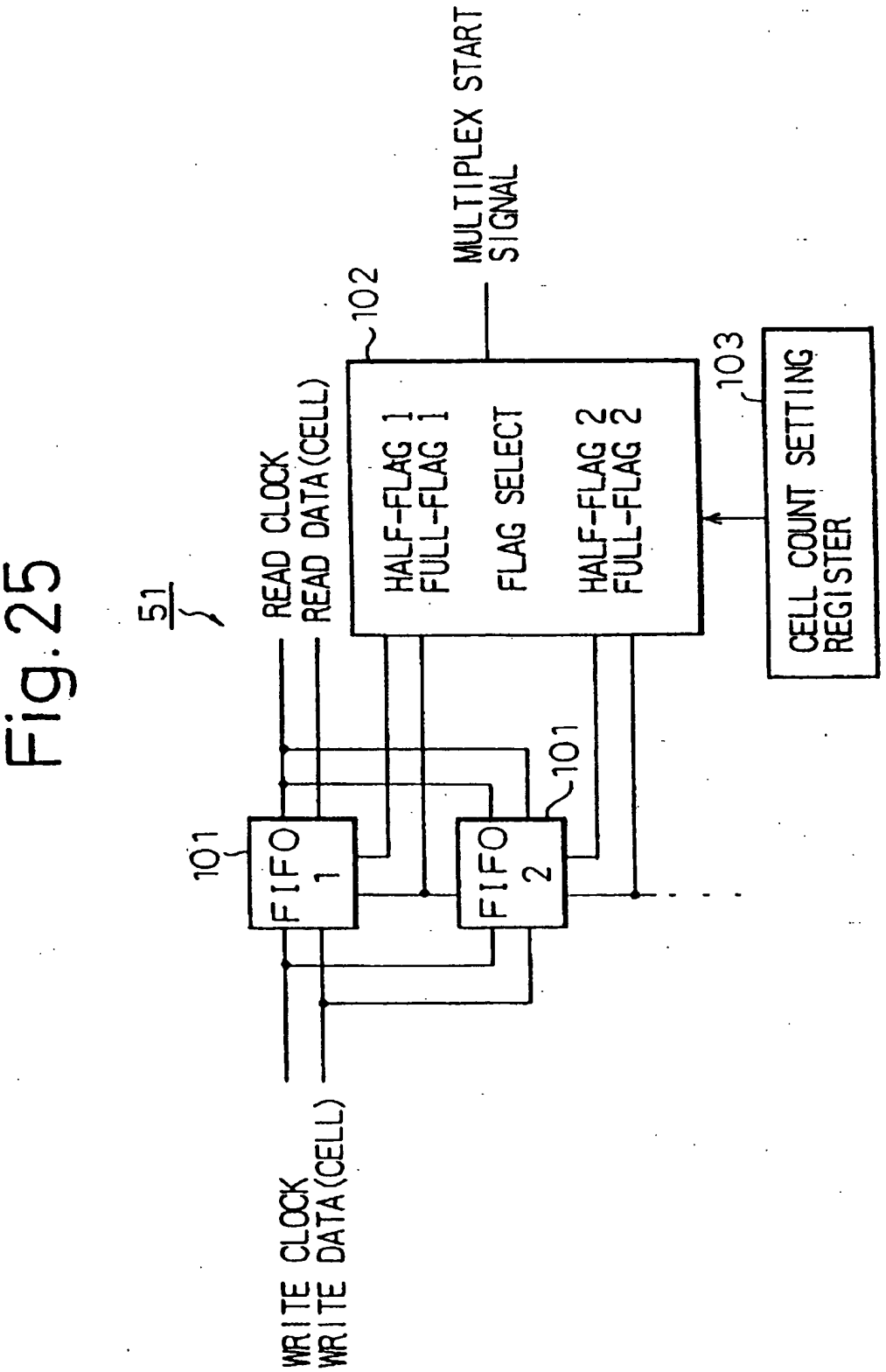
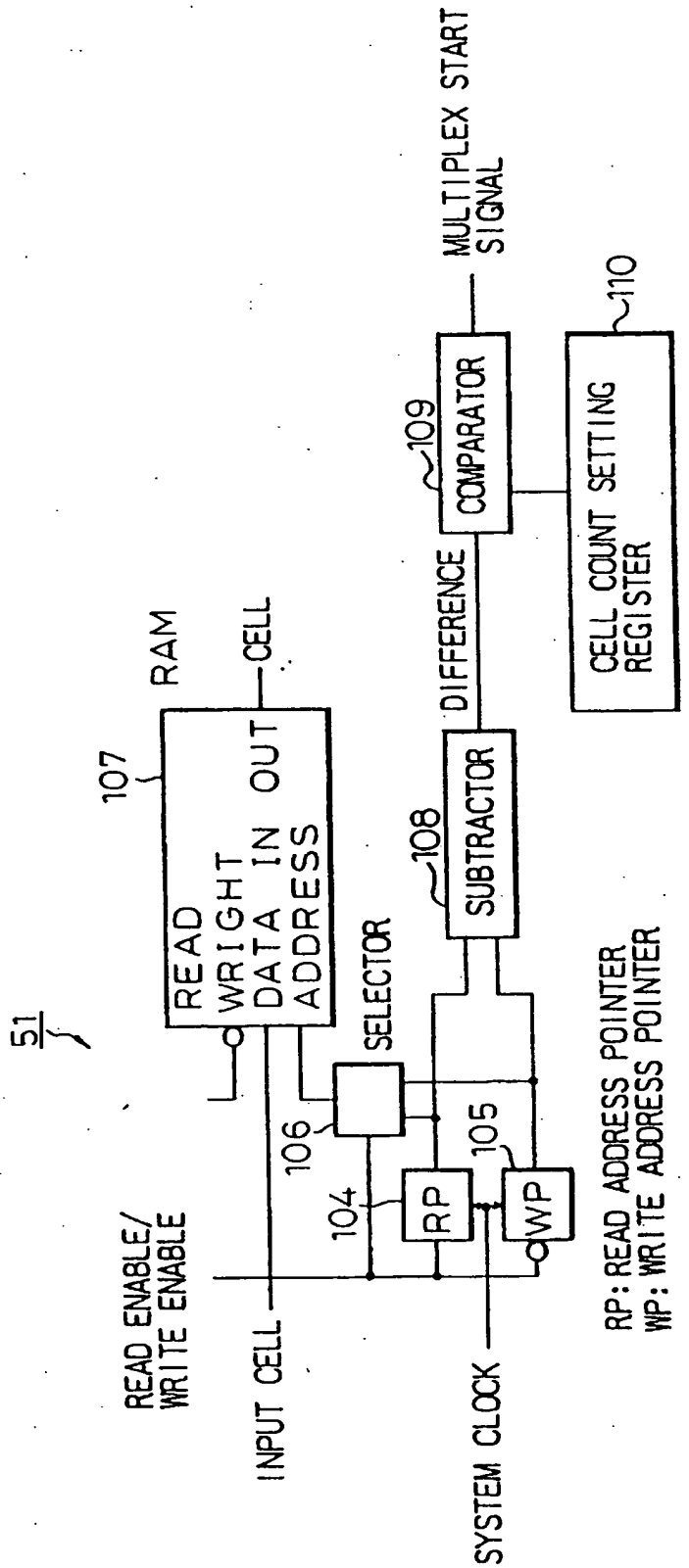

51
READ CLOCK
READ DATA(CELL)
WRITE CLOCK
WRITE DATA(CELL)
MULTIPLEX START SIGNAL
102
HALF-FLAG 1
FULL-FLAG 1
FLAG SELECT
HALF-FLAG 2
FULL-FLAG 2
103
CELL COUNT SETTING REGISTER
101
FIFO 1
101
FIFO 2
101

Fig.26


51
RAM
107
READ
WRIGHT
DATA IN
ADDRESS
OUT
CELL
SELECTOR
106
104
RP
105
WP
108
SUBTRACTOR
DIFFERENCE
109
COMPARATOR
MULTIPLEX START SIGNAL
110
CELL COUNT SETTING REGISTER
READ ENABLE/ WRITE ENABLE
INPUT CELL
SYSTEM CLOCK
RP: READ ADDRESS POINTER
WP: WRITE ADDRESS POINTER

CELL MULTIPLEXING APPARATUS IN ATM NETWORK

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a cell multiplexing apparatus for asynchronous transfer mode (ATM) communication, and more particularly to a cell multiplexing apparatus for multiplexing cells having different virtual path identifiers (VPIs) along the same path into one multiplexed cell at a node-to-network interface (NNI). In this specification, cell multiplexing means multiplexing information cells from a plurality of channels into one cell.

2. Description of the Related Art

In recent years, B-ISDN (Broadband Integrated-Services Digital Network) has emerged as the next generation public network, and with the implementation of the B-ISDN, even more flexible broadband communication networks are being realized which can provide such services as voice communications, very high-speed file transfer, information communications, communications between LANs, moving image transmission, and even moving image services for high-definition television (HDTV). ATM communication technology that can handle such multimedia is used in B-ISDN.

In ATM communication, high-speed asynchronous transmission is performed using ATM cells, and when communication path congestion is encountered, the CLP control bit in each ATM cell is checked and ATM cells whose CLPs are "1" are preferentially discarded. Further, cell multiplexing is performed to prevent such communication path congestion and also to increase cell utilization. For example, when transmitting voice cells constructed by assembling PCM voice code data at 64 Kb/s into ATM cells, the amount of voice data that can be carried in one voice cell is limited because of the associated time delay; as an example, if the allowable delay time is 0.5 ms, voice information that can be carried in one voice cell is only four bytes of data, i.e., 0.5 ms (delay time) / 125 μs (8 kHz sampling)=4 samples.

The above technique of cell multiplexing is such that in transmission of voice cells of a plurality of voice channels, if the cells have the same VPI between them, the voice information carried in these cells is merged and stored in an information field of one multiplexed cell, and a VPI common to the voice channels is appended to the VPI of the multiplexed cell for transmission. For example, if one cell can contain 40-octets of user information, it follows that in the above example, voice information for 10 channels (10 voice cells) can be combined into one multiplexed cell. Thus, the probability of occurrence of communication path congestion decreases because of the reduced number of voice cells (from 10 voice cells to one multiplexed cell). Furthermore, since voice information for multiple channels is carried in one multiplexed cell for transmission, cell utilization increases with an increasing degree of multiplexing (utilization of the information field is increased from four octets to 40 octets).

The above-described cell multiplexing has been known in the prior art, i.e, a plurality of cells having the same VPI for transmission along the same path from an user network interface (UNI) is assembled into one multiplexed cell. However, it has not been practiced to multiplex cells with different VPIs into one multiplexed cell at each node in an ATM network; the only technique employed to handle such a situation has been the so-called statistical multiplexing whereby the cells are simply distributed to the paths designated by their VPIs (empty cells used for cell synchronization within the network are asynchronously replaced by information cells). This is because when the VPIs are different, the paths over which the cells are to be transmitted may be different. Suppose that, in such a case, the above-described cell multiplexing were performed unconditionally at each communication node without checking the identity of the VPIs. Then, the intermediate node that received the multiplexed cell would have to disassemble the multiplexed cell, determine the destination of each individual cell contained in the 10 multiplexed cell, and then reassemble the cells into a multiplexed cell for transmission. This would not only increase the transmission delay associated with cell multiplexing but also add to the load at each node.

However, the VPI of each cell is usually assigned for each user network interface (UNI), and there are cases in which different VPIs from different UNIs may designate the same path. Furthermore, when the number of channels designated by one VPI is increased, different VPIs may be assigned to designate the same path from the standpoint of network management. This is also true when the number of user network interfaces (UNIs) connected to the network is increased (which is equivalent to increasing the number of channels). In these cases, the VPIs of individual cells are different but designate the same path, and no problems occur with the above cell multiplexing. Furthermore, since these cases arise due to increased number of channels, etc., as noted above, by positively utilizing the technique of cell multiplexing the effects of cell multiplexing, such as reducing the possibility of congestion and increasing the cell utilization efficiency, can be further enhanced.

SUMMARY OF THE INVENTION

It is accordingly an object of the invention to provide a cell multiplexing apparatus wherein, using a facility for managing the VPIs of the cells intended for transmission along the same path, the assignment of the VPIs between NNIs is controlled so that the cells intended for transmission along the same path are multiplexed by assigning a representative VPI representing these cells even when the cells have different VPIs between them.

It is another object of the invention to provide a cell multiplexing apparatus wherein a facility for predicting the occurrence of congestion is added to the above-described cell multiplexing apparatus and, in order to reduce cell transmission delays, cell multiplexing is usually not performed, but performed only when the occurrence of congestion is predicted.

According to the present invention, there is provided a cell multiplexing apparatus in an ATM network, comprising: transmitting means 1 in which the information fields of a plurality of ATM cells intended for transmission along the same path are multiplexed and stored into an information field of one multiplexed cell and a representative VPI globally representing the VPIs, including different VPIs, of the plurality of ATM cells intended for transmission along the same path is assigned as the VPI of the multiplexed cell for transmission; and receiving means 2 in which the representative VPI is detected from received cells and the plurality of ATM cells having individual VPIs and transmitted along the same path are reconstructed from the multiplexed cell having the representative VPI.

In one mode of the invention, the VPI area of the ATM header of the multiplexed cell is divided into two segments so that the representative VPI is carried in one segment and

VPI information of the plurality of ATM cells intended for transmission along the same path is carried in the other segment, and the path distribution for the multiplexed cell is done in accordance with the representative VPI; further, the transmitting means 1 includes congestion predicting means for predicting the occurrence of congestion from the relationship between the number of input cells and the number of output cells, and the multiplexed cell is assembled and sent out only when the occurrence of congestion is predicted.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be more clearly understood from the description as set forth below with reference to the accompanying drawings wherein:

FIG. 1 is a diagram showing an example of an ATM network configuration;

FIG. 2 is a diagram showing the structure of an ATM cell at NNI;

FIG. 3 is a diagram showing the structure of an ATM cell at UNI;

FIG. 4 is a diagram showing an example of a multiplexed cell assembled by multiplexing voice cells;

FIG. 5 is a block diagram showing the basic configuration of a transmitting section in a cell multiplexing apparatus according to the present invention;

FIG. 6 is a block diagram showing the basic configuration of a receiving section in the cell multiplexing apparatus according to the present invention;

FIG. 7 is a diagram for explaining a representative VPI (1) according to the present invention;

FIG. 8 is a diagram for explaining a representative VPI (2) according to the present invention;

FIG. 9 is a diagram showing an example of an ATM network employing the cell multiplexing apparatus according to the present invention;

FIG. 10 is a diagram showing an embodiment of the transmitting section in the cell multiplexing apparatus according to the present invention;

FIG. 11 is a diagram for explaining the operation of a detector at the transmitting side when the representative VPI (1) shown in FIG. 7 is used;

FIG. 12 is a diagram for explaining the operation of the detector at the transmitting side when the representative VPI (2) shown in FIG. 8 is used;

FIG. 13 is a diagram showing an example of the functional configuration of a multiplexer when the representative VPI (1) shown in FIG. 7 is used;

FIG. 14 is a diagram showing an example of a control flow for FIG. 13;

FIG. 15 is a diagram showing an example of the functional configuration of the multiplexer when the representative VPI (2) shown in FIG. 8 is used;

FIG. 16 is a diagram showing an example of a control flow for FIG. 15;

FIG. 17 is a diagram showing an embodiment of the receiving section in the cell multiplexing apparatus according to the present invention;

FIG. 18 is a diagram for explaining the operation of a detector at the receiving side when the representative VPI (1) shown in FIG. 7 is used;

FIG. 19 is a diagram for explaining the operation of the detector at the receiving side when the representative VPI (2) shown in FIG. 8 is used;

FIG. 20 is a diagram showing an example of the functional configuration of a demultiplexer when the representative VPI (1) shown in FIG. 7 is used;

FIG. 21 is a diagram showing an example of a control flow for FIG. 20;

FIG. 22 is a diagram showing an example of the functional configuration of the demultiplexer when the representative VPI (2) shown in FIG. 8 is used;

FIG. 23 is a diagram showing an example of a control flow for FIG. 22;

FIG. 24 is a diagram showing an embodiment in which each input buffer in the transmitting section is provided with a congestion prediction function;

FIG. 25 is a diagram showing an example in which each buffer shown in FIG. 24 is constructed from a FIFO memory; and

FIG. 26 is a diagram showing an example in which each buffer shown in FIG. 24 is constructed from a RAM.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Before describing the preferred embodiments according to the present invention, examples of the related art are provided with reference to accompanying drawings FIGS. 1 to 4.

FIG. 1 is a schematic diagram illustrating how communications are performed between nodes in a B-ISDN.

In FIG. 1, user terminals 131 are connected to communication nodes 132 via respective user network interfaces (UNIs). High speed asynchronous transmission using ATM cells is performed between the communication nodes via node-to-network interfaces (NNIs) and digital service units (DSUs). Each communication node 132 contains ATM adaptation layers (AALs) 133 and ATM switches 134. The AAL 133 is responsible for ATM cell assembly and disassembly between the user terminal 131 and the ATM switch 134. Data from the user terminal 131 is broken up into a plurality of ATM cells which are then transferred via the ATM switch 134.

FIGS. 2 and 3 show examples of ATM cells. The former (FIG. 2) shows the format of the NNI which is an interface between the communication nodes 132, and the latter (FIG. 3) shows the format of the UNI which is an interface between the user terminal 131 and the communication node 132. Each ATM cell consists of 53 octets, of which the first five octets represents the ATM header designating the communication destination and the remaining 48 octets constitute the information field carrying packetized voice, data, etc. from the terminal.

The ATM header contains a virtual path identifier (VPI) that specifies a communication path, a virtual channel identifier (VCI) that specifies a channel to be used in the specified communication path, control bits such as PT (payload type) and CLP (cell loss priority), and a CRC calculation value for HEC (header error control). The information field carries information from the terminal, such as voice, data, etc. that has been assembled into cells of 48 octets. If the information does not fill up to the 48 octets, any remainder is filled with blanks. The UNI (FIG. 3) is provided with a generic flow control (GFC) facility. The GFC is used to control contention between cells on the same physical layer connection when a plurality of terminals are connected to the user side of the UNI. The GFC is therefore not provided in the NNI (FIG. 2).

Referring back to FIG. 1, data from each terminal **131** is assembled into cells by the AAL **133** and a communication path is set up by the ATM switch **134**. Using the header data in each ATM cell, the ATM switch **134** performs the high speed switching operation by hardware which is the feature of ATM. FIG. **1** illustrates how the user terminals **131** connected to the respective communication nodes **132** communicate with each other over communication paths, i.e. virtual paths (VPs) **136** and virtual channels (VCs) **137** specified therein. If communication path congestion is detected by the ATM switch section **134** during communication, the ATM switch **134** discards part of the data transmitted from the transmitting user terminal **131**. In this case, the ATM switch **134** checks the CLP control bit in the ATM cell format (FIGS. **2**, **3**) and preferentially discards cells whose CLP value is "1".

Cell multiplexing is performed to avoid congestion of the communication path and also to increase cell utilization. For example, when transmitting voice cells constructed by assembling PCM voice code data of 64 Kb/s into ATM cells, the amount of voice data that can be carried in one voice cell is limited because of the associated time delay; as an example, if the allowable delay time is 0.5 ms, the voice information that can be carried in one voice cell is only four bytes of data, i.e., 0.5 ms (delay time) / 125 μs (8 kHz sampling)=4 samples. The above technique of cell multiplexing is such that in transmission of voice cells of a plurality of voice channels, if the cells have the same VPI between them, the voice information carried in these cells is merged and stored in an information field of one multiplexed cell, and a VPI common to the voice channels is appended to the VPI of the multiplexed cell for transmission. For example, if one cell can contain 40-octets of user information, it follows that in the above example, voice information of 10 channels (10 voice cells) can be combined into one multiplexed cell. Thus, the probability of occurrence of communication path congestion decreases because of the reduced number of voice cells (from 10 voice cells to one multiplexed cell). Furthermore, since voice information of multiple channels is carried in one multiplexed cell for transmission, cell utilization increases with increasing degree of multiplexing (utilization of the information field is increased from four octets to 40 octets).

FIG. **4** illustrates an example of a multiplexed cell assembled by multiplexing voice cells such as described above. As described, the information field of the multiplexed cell accommodates the voice information of a plurality of channels that number n (n is an integer), while the control information field thereof contains, for example, address information to identify the location of each of the plurality of voice information items stored (channels 1 to n), and control information used to disassemble the multiplexed cell and reassemble the individual voice cells at the destination node. A VPI common to the plurality of channels is written in the ATM header.

The preferred embodiments of the present invention will now be described below.

FIG. **5** is a block diagram showing the basic configuration of a transmitting section in a cell multiplexing apparatus according to the present invention.

As shown in FIG. **5**, transmitting means **1** comprises: input buffer means **13** for buffering a prescribed number of incoming cells; VPI managing means **11** for managing the VPIs of a plurality of ATM cells to be transmitted along the same path; representative VPI assigning means **12** for assigning a representative VPI representing the VPIs of the plurality of ATM cells to be transmitted along the same path; path match detecting means **14** for comparing the VPIs of the incoming cells output from the input buffer means **13** with the VPIs for the same path supplied from the VPI managing means **11**, and for separating the incoming cells into matched cells for which the VPIs match and unmatched cells for which the VPIs do not match; multiplexed cell assembling means **15** for assembling a plurality of matched cells supplied from the path match detecting circuit **14** into one multiplexed cell, and for assigning the representative VPI from the representative VPI assigning means **12** as the VPI of the multiplexed cell; and output buffer means **16** for buffering the multiplexed cells from the multiplexed cell assembling means **15** and/or the unmatched cells from the path match detecting means **14**.

The input buffer means **13** temporarily stores incoming cells, and when the number of incoming cells stored therein exceeds a prescribed value, it is decided that congestion is most likely to occur, and a congestion prediction signal is issued. The VPI managing means **11** manages the VPIs of a plurality of cells to be transmitted along the same path, including such cells as having different VPIs, while the representative VPI assigning means **12** assigns a representative VPI globally representing the VPIs of the plurality of cells to be transmitted along the same path. The path match detecting means **14** compares the VPI of each of the incoming cells transferred from the input buffer means **13** with the VPIs for the same path supplied from the VPI managing means **11**, and separates the incoming cells into matched cells for transmission along the same path and unmatched cells for transmission along different paths.

The cells to be transmitted along the same path are supplied to the multiplexed cell assembling means **15** at the next stage, where the information fields of these cells are combined together and assembled into a multiplexed cell to which the representative VPI supplied from the VPI assigning means **12** is appended. The output buffer means **16** buffers the multiplexed cell supplied from the multiplexed cell assembling means **15** for transmission along the same path and the individual cells supplied from the path match detecting means **14** for transmission along different paths, and outputs them at prescribed timing.

FIG. **6** is a block diagram showing the basic configuration of a receiving section in the cell multiplexing apparatus according to the present invention.

As shown in FIG. **6**, receiving means **2** comprises: input buffer means **23** for buffering a prescribed number of received cells; representative VPI assigning means **21** for assigning a representative VPI for a multiplexed cell assembled from a plurality of ATM cells to be transmitted along the same path; VPI managing means **22** for managing the VPIs of the plurality of ATM cells assembled into the multiplexed cell; representative VPI detecting means **24** for comparing the VPIs of the received cells supplied from the input buffer means **23** with the representative VPI supplied from the representative VPI assigning means **21**, and for separating the received cells into multiplexed cells each with a representative VPI for which the VPIs match and the other received cells for which the VPIs do not match; multiplexed cell disassembling means **25** for disassembling each matched multiplexed cells supplied from the representative VPI detecting means **24** into their component ATM cells; and output buffer means **26** for buffering the ATM cells supplied from the multiplexed cell disassembling means **25** and/or the unmatched received cells supplied from the representative VPI detecting means **24**.

The input buffer means **23** buffers received cells and supplies them to the representative VPI detecting means **24**

at the next stage. The representative VPI assigning means 21 and the VPI managing means 22 have functions equivalent to those of the representative VPI assigning means 12 and the VPI managing means 11 in the transmitting means 1. The representative VPI detecting means 24 separates the received cells into cells having representative VPIs and the other cells, and outputs them separately. The multiplexed cell disassembling means 25 reconstructs the individual ATM cells having original VPIs, from the information contained in the information field of the received cell having the representative VPI and also from the information supplied from the VPI managing means 22. The output buffer means 26 buffers the reconstructed ATM cells and the cells having no representative VPIs, and holds them for output.

FIGS. 7 and 8 each show a schematic diagram for explaining the construction of a representative VPI according to the present invention.

In FIG. 7, a representative VPI 34 (table address Y_0) is written into the ATM header 31 of an ATM cell in accordance with a VPI management table 33 contained in the VPI managing means 11 of the transmitting means 1 (FIG. 5), and individual VPI information designated by the representative VPI is written into the information field 32 of the ATM cell along with the contents of the information field of each cell multiplexed. For the individual VPI information 35, individual VPI numbers (VPI #121, VPI #122, etc. shown in FIG. 7) may be written directly, or instead, identifying information for identifying them (e.g., corresponding table addresses Y_1–Y_n) may be written.

In the receiving means 2 (FIG. 6), the representative VPI detecting means 24 detects the representative VPI 34 from the ATM header 31 of the received cell, and the individual ATM cells are reconstructed from the individual VPI information 35 (VPI #121, VPI #122, etc.) contained in the information field 32, or from the identifying information (Y_1–Y_n) by using the VPI management table 33 contained in the VPI managing means 22, as is done at the transmitting side.

According to the format of FIG. 7, it is possible to reconstruct individual ATM cells just by identifying the representative VPI number at the receiving side, in which case the VPI management table can be simplified. Furthermore, this format can be used in connectionless communications.

FIG. 8 shows the format in which the VPI area of the NNI format in the ATM header 31 is divided into two segments, one segment (which, in FIG. 8, corresponds to the GFC area (AAAA) in the UNI format) being allocated to a representative VPI and the remaining VPI area being allocated bit by bit (X_0–X_7) to the VPI information of the cells multiplexed. Since the GFC area is not used in communications between nodes, assigning the representative VPI of the invention to that area helps to maintain consistency with existing networks.

As shown in the right side of FIG. 8, AAAA=0 indicates that the cell is a normal cell that has not been multiplexed. Therefore, in the case of FIG. 8, a total of 15 representative VPIs from AAAA=1 to AAAA=15 are available for selection. Each of the VPI numbers 1 to 15 corresponds to one of 15 VPI management tables (37-1 to 37-15). The bits X_0–X_7 in each representative VPI corresponds to eight addresses in the associated VPI management table. Any one of the bits X_0–X_7 that is set to "1" indicates that the individual VPI stored at the corresponding address is used. For example, when AAAA=0010 and X_7–X_8=00000011, as shown in FIG. 8, it indicates that the representative VPI #2 is comprised of two individual VPIs #121 and #122.

The format of FIG. 8 requires the provision of representative VPIs and VPI management tables containing corresponding individual VPI information at both the transmitting and receiving sides, but since the amount of VPI information carried in a multiplexed cell is small and the processing at intermediate nodes, etc. is therefore simplified, this format has the advantage of minimizing processing time delays, etc. Furthermore, since the mapping between the representative VPIs and the groups of individual VPIs is simple, the format has the further advantage that hardware implementation is easy, thereby allowing high-speed VPI retrieval, etc.

FIG. 9 shows an example of an ATM network in which the cell multiplexing apparatus of the invention is employed.

In FIG. 9, B-ISDN terminals (B-NT) 41 are connected to an ATM exchange (1) 42 via user network interfaces UNIs. The ATM exchange (1) 42 multiplexes ATM cells having VPI #121 and #122 designating transmission along the same path, and appends a representative VPI #12 to the multiplexed cell for transmission. The number #12 of the representative VPI indicates that this representative VPI designates the path leading from the ATM exchange (1) to the next ATM exchange (2). For other paths, for example, a VPI #131 designating the path leading to an ATM exchange (3) in the case of FIG. 9, cells are not multiplexed but sent out as normal ATM cells.

In the ATM exchange (2) 43, upon detecting the representative VPI #12, the individual ATM cells having the original VPIs #121 and #122 are reconstructed from the individual VPI information carried in the information field of the ATM cell having the representative VPI #12, or by referencing the VPI information contained in the VPI management table corresponding to the representative VPI #12, as described previously in connection with FIGS. 7 and 8. The reconstructed cells are then transferred to B-ISDN terminals (B-NT) 44 via respective user network interfaces UNIs. The cells with the VPI #131 designating the different path are relayed as are. In the example shown in FIG. 9, a B-ISDN terminal (B-NT) 45 is connected to the ATM exchange (2) 43 via a user network interface. Since its path VPI #231 designates the same path as the above path VPI #131, the cells can be multiplexed together as in the previous example, but FIG. 9 shows an example in which the ATM exchange (2) 43 judges that the situation does not lead to congestion of the communication path leading to the ATM exchange (3) 46, so that the cells are not multiplexed in this case.

FIG. 10 is a block diagram showing one embodiment of the transmitting section in the cell multiplexing apparatus according to the present invention.

In comparison with the invention shown in FIG. 5, the buffers 51 shown in FIG. 10 correspond to the input buffer means 13 of FIG. 5, and the VPI management table 53 and VPI assignment functional section 54 shown in FIG. 10 correspond to the VPI managing means 11 and representative VPI assigning means 12, respectively, shown in FIG. 5. Further, the path distributor 52 and detector 55 shown in FIG. 10 together correspond to the path match detecting means 14. The multiplexer 56 in FIG. 10 corresponds to the multiplexed cell assembling means 15 of FIG. 5, and the buffer 57 shown in FIG. 10 corresponds to the output buffer means 16 of FIG. 5.

In FIG. 10, assuming that the transmitting section 50 is used in the ATM exchange (1) shown in FIG. 9, the ATM cells received from the B-ISDN terminals 41 are input to the buffers 51 according to their path VPIs #121, #122, and #131. Using VPI tables containing fixed values stored at the

time of system setup or variable values stored at the time of path setup to the destination, the VPI management table 53 controls the path distributor 52 comprised of ATM switches and distributes the incoming cells to the respective common paths (#12X, #13X, etc.).

In the detector 55, the VPI numbers of the distributed cells are compared with the VPI numbers supplied from the VPI management table 53 for multiplexing onto the designated path; the cells for which the VPI numbers match are transferred to the multiplexer 56 at the next stage, while the cells for which the VPI numbers do not match are passed directly to the buffer 57. In the example shown in FIG. 10, VPI #121 and VPI #122 are given from the VPI management table 53 as the VPI group to be multiplexed, so that the incoming cells having the VPI #121 or #122 are transferred to the multiplexer 56 as matched cells. The VPI assignment functional section 54 supplies the representative VPI number (VPI #12) representing the multiplex VPI group to the multiplexer 56. The multiplexer 56 then assembles a multiplexed cell with the representative VPI written to the VPI field of its ATM header and the information contents of the matched cells written to its information field, and transfers the thus assembled multiplexed cell to the buffer 57 at the next stage. The buffer 57 also holds the non-multiplexed cells directly passed from the detector 55, and the multiplexed and non-multiplexed cells are sequentially output at the prescribed cell transmit timing.

FIG. 11 is a diagram for explaining the operation of the detector 55 when the representative VPI (1) shown in FIG. 7 is used.

The example of FIG. 11 shows a case in which an ATM cell having the VPI #122 arrives and the VPI (#122) carried in its ATM header is input to a register 61. A comparator 62 compares the VPI held in the register 61 with each VPI stored in the VPI management table 53, and detects a match with #122 at table address X1, upon which a switch 63 at the subsequent stage is set to connect to the multiplexer 56. At the same time, the representative VPI #12 stored at address X_0 in the VPI management table 53 is supplied to the multiplexer 56.

FIG. 12 is a diagram illustrating, as an alternative example, the operation of the detector 55 when the representative VPI (2) shown in FIG. 8 is used.

The process of FIG. 12 is the same as that shown in FIG. 11 up to the step where the VPI #122 is detected. In FIG. 12, the representative VPI and individual VPI information given to the multiplexer 56 are different from those described in FIG. 11. That is, for the representative VPI, a four-bit table number AAAA=0010 stored in the VPI management table 2 is given, and for individual VPI information X_0-X_1, an identifier X_1=1 indicating the use of the VPI #122 is given.

Next, the operation of the multiplexer 56 will be described with reference to FIGS. 13 and 14 and FIGS. 15 and 16. The functional configuration shown in FIG. 13 and the control flow shown in FIG. 14 are related to FIG. 11 and concern the operation of the multiplexer 56 when the representative VPI (1) shown in FIG. 7 is used. On the other hand, the functional configuration shown in FIG. 15 and the control flow shown in FIG. 16 are related to FIG. 12 and concern the operation of the multiplexer 56 when the representative VPI (2) shown in FIG. 8 is used.

The detector 55 shown in the left side of FIG. 13 has already been described with reference to FIG. 11, and therefore, the description thereof will not be repeated here. When a match is detected by the comparator 62, a gate circuit 64 (which corresponds to the VPI assignment functional section 54 of FIG. 10) is enabled for output so that the representative VPI #12 stored at address X_0 is written into the ATM header of a multiplex buffer 70. Upon the detection of the match, the ATM cells (VPI #121, VPI #122) to be multiplexed are each directed via the switch 63 to a VPI separator 65 where each cell is disassembled to separate the VPI field from the information field; the separated VPI field and information field are then written into a VPI storing area and an information field storing area, respectively, in the information field of the multiplex buffer 70. For the VPI information written into the VPI storing area, the VPI number of each ATM cell may be written directly, as shown in FIG. 13, or instead, an identifier, i.e. the information identifying an address in the VPI management table, may be written.

A timer 68, which operates with the system clock, starts counting at the instant in time when the first cell is written into the multiplex buffer 70, and outputs a count end signal at the end of a prescribed time. The prescribed time is set equal to the multiplex processing time allowed for cell multiplexing within the previously noted allowable voice delay time. A counter 66 counts up on a cell write clock for every cell write, and outputs a signal when a prescribed number of cells have been multiplexed. A register 67 is used to set the multiplexing delay time for the timer 68 and the number of cells to be multiplexed for the counter 66, thereby controlling the cell multiplexing in the multiplex buffer 70. An OR circuit 69 outputs an output signal from either the timer 68 or the counter 66 as an output enable signal to the multiplex buffer 70. Upon reception of the output enable signal, the multiplex buffer 70 outputs a multiplexed cell assembled up to that time.

FIG. 14 shows an example of a control flow for FIG. 13.

In FIG. 14, steps S101 and S102 concern the operation of the detector 55, where the VPI of each incoming cell is compared with the VPIs stored in the VPI management table. When a match is found as a result of the comparison, then the process proceeds to step S103 and on to the subsequent steps, which concern the operation of the multiplexer 56. First, the representative VPI is written into the VPI area in the multiplex buffer 70 (S103). Then, the VPI information (VPI number or VPI identifier) and the contents of the information field of the cell are written into the VPI storing area and information field storing area, respectively, in the multiplex buffer 70 (S104, S105). The counter 66 is incremented by the write signal (S106). The timer 68 is already started in step S102 upon the detection of the match.

In step S107, the counter 66, the timer 68, and the multiplex buffer 70 are checked as to whether they have finished counting or become full. If not full (NO), the process returns to step S101 to process the next incoming cell for multiplexing; the number of cells multiplexed thus increases. When the full state is detected in step S107 (YES), the multiplexed cell assembled from the cells multiplexed up to that time is output, thus completing the multiplexing operation (S108, S109). On the other hand, if no match is found in step S102, the multiplexing operation is not performed and the normal ATM cell is output as is (S110, S111).

Now, using the functional configuration of FIG. 15 and the control flow of FIG. 16, the operation of the multiplexer 56 will be described below when the representative VPI (2) shown in FIG. 8 and related to FIG. 12 is used.

The configuration shown in FIG. 15 is substantially the same as that shown in FIG. 13; in FIG. 15, corresponding parts to those shown in FIG. 13 are designated by the same reference numerals, and the descriptions of such parts are

not repeated here. As described with reference to FIG. 8, when the detector 55 detects a match between the representative VPI (high-order four bits) of the incoming cell and the number of the VPI management table 53, the representative VPI (AAAA) corresponding to the VPI management table number is written via the gate circuit 64 into the first four bits (GFC area) in the ATM header of the multiplex buffer 70. When the VPI (high-order four bits) of the incoming cell is not all 0, these four bits may be directly transmitted as the representative VPI.

For individual VPI information, flag information corresponding to the memory address of each individual VPI number written in the VPI management table (1 is set in address X_0–X_1 where the VPI address is written) is written into the next eight-bit area (VPI area) after the first four bits (GFC area) in the multiplex buffer 70 shown in FIG. 15. In the case of FIG. 15, since the VPI information of each cell to be multiplexed is managed by the VPI management table provided in each transmit/receive node, the VPI separator 65 and the VPI storing area in the multiplex buffer 70 used in the configuration shown in FIG. 13 need not be provided.

FIG. 16 shows a control flow for FIG. 15. The control flow shown in FIG. 16 is substantially the same as that shown in FIG. 14, except that the contents of steps S203 through S205 in FIG. 16 are different from those of steps S103 through S105 in FIG. 14.

In step S203, the VPI management table number (AAAA) is written into the GFC area in the multiplex buffer, as described above, and in step S204, address flags X_0–X_7 corresponding to matched VPIs are set to 1. Then, in step S205, only the information field of the input cell is written into the information field of the multiplex buffer 70.

FIG. 17 is a block diagram showing one embodiment of the receiving section in the cell multiplexing apparatus according to the present invention.

In comparison with the invention shown in FIG. 6, the buffers 81 shown in FIG. 17 correspond to the input buffer means 23 of FIG. 6, and the VPI management table 83 and VPI assignment functional section 86 shown in FIG. 17 correspond to the VPI managing means 22 and representative VPI assigning means 21, respectively, shown in FIG. 6. Further, the path distributor 82 and detector 84 shown in FIG. 17 together correspond to the representative VPI detecting means 24 shown in FIG. 6. The demultiplexer 85 shown in FIG. 17 corresponds to the multiplexed cell disassembling means 25 of FIG. 6, and the buffer 87 shown in FIG. 17 corresponds to the output buffer means 26 of FIG. 6.

In FIG. 17, assuming that the receiving section 80 is used in the ATM exchange (2) shown in FIG. 9, the received cells (respectively having VPI #12, VPI #131, and VPI #231) temporarily held in the buffers 81 are distributed to the respective paths by means of the path distributor 82 controlled by the VPI management table 83, as in the case of the previously-described transmitting section (FIG. 10). The detector 84 detects the representative VPI carried in the ATM header of each received cell to distinguish the multiplexed cell (VPI #12) transmitted from the transmitting section. Each cell having the representative VPI #12 is reconstructed into the original individual ATM cells (VPI #121, VPI #122) by the demultiplexer 85 at the next stage. The reconstructed ATM cells and the non-multiplexed normal cells are buffered in the buffer 87 which outputs each cell onto the path designated by the VPI of the cell at the prescribed cell transmit timing.

FIG. 18 is a diagram illustrating the operation of the detector 84 when the representative VPI (1) shown in FIG. 7 is used.

In FIG. 18, the VPI area in the ATM header of each received cell is input to a shift register 91 in the detector 84. A comparator 92 in the detector 84 compares the VPI held in the shift register 91 with the representative VPI supplied from the VPI management table 83; when they match, the cell is determined as a multiplexed cell and a switch 93 at the subsequent stage is set to connect to the demultiplexer 85. In the example shown, the representative VPI #12 is input to the shift register 91, and a match is found with the representative VPI #12 stored at address X_0 in the VPI management table 83.

When the representative VPI format (1) shown in FIG. 7 is used, the VPI information of each individual cell is either directly written in the information field of the multiplexed cell or identified by an address identifier contained in the VPI management table 83, as previously described. In the former case, individual ATM cells can be reconstructed directly from the received cell by the demultiplexer 85, and in the latter case, the VPI #122 contained in the VPI management table 83 can be obtained using the address identifier X_1, as shown by a dotted line in FIG. 18.

FIG. 19 is a diagram illustrating, as an alternative example, the operation of the detector 84 when the representative VPI format (2) is used.

In FIG. 19, the GFC area consisting of the first four bits input to the shift register 91 is examined to determine whether the cell is a multiplexed cell or not (cells other than AAAA=0000 are multiplexed cells). The representative VPI number indicated by the first four bits refers to the corresponding VPI management table number (1–15), and the value of each remaining VPI bit (X_0–X_1) indicates the corresponding memory address in the table. Therefore, each individual VPI information can be readily obtained using these bits. In the example shown, the VPI management table number 2 is obtained from the representative VPI #2 of the received cell, and since the remaining received VPI bits are X_0–X_7=11000000, the individual VPI information designated by the representative VPI is obtained from address X_0 and address X_1 in the VPI management table number 2 (VPI #121 and VPI #122).

Next, the operation of the demultiplexer 85 will be described with reference to FIGS. 20 and 21 and FIGS. 22 and 23. The functional configuration shown in FIG. 20 and the control flow in FIG. 21 are related to FIG. 18 and concern the operation of the demultiplexer 85 when the representative VPI (1) shown in FIG. 7 is used. The functional configuration shown in FIG. 22 and the control flow in FIG. 23 are related to FIG. 19 and concern the operation of the demultiplexer 85 when the representative VPI (2) shown in FIG. 8 is used.

The detector 84 shown in the left side of FIG. 20 has already been described with reference to FIG. 18, and therefore, the description thereof will not be repeated here. When a match is detected by the comparator 92 with the representative VPI #12, the multiplexed cell for which the match was detected is written into a multiplex buffer 94 in the demultiplexer 85 via a switch 93. When the multiplexed cell is written into the multiplex buffer 94, a read/write circuit 95 reads out data of the multiplexed VPI storing areas and information field storing areas from the information field, and sequentially writes the data into the cell buffers, 96, 97, . . . , each constructed with a shift register. For example, VPI #121 and VPI #122 read from the VPI storing areas are written into the ATM headers of the cell buffers 96 and 97, respectively, and their corresponding cell information read from the information field storing areas is written

into the information fields of the respective buffers. Each ATM cell thus reconstructed is sequentially clocked out of the shift register and fed to a buffer **87** at the output stage.

The above blocks are reset after the cells are output from the cell buffers **96, 97,** . . . If a pointer facility is provided to the cell buffers, the above blocks can be reset at the instant in time when the data are written into the cell buffers. A pointer facility is used to indicate the shift position in a shift register, i.e., data position within a shift register. By using this, read/write operations can be started at the address location next to the pointer; therefore, there is no need to wait until the data are output from the cell buffers. This has the effect of reducing delays, etc.

FIG. **21** shows an example of a control flow for FIG. **20** described above.

In FIG. **21**, steps **S301** and **S302** concern the operation of the detector **84**, where the VPI of each received cell is compared with the VPIs contained in the VPI management table. When a match is found, the process proceeds to step **S303** and on to the subsequent steps, which concern the operation of the demultiplexer **85**. First, the received cell is written into the multiplex buffer **94** (**S303**). Next, the individual ATM cell information read out of the VPI storing area and information field storing area of the multiplex buffer is written into the ATM header and information field in the respective cell buffers **96, 97,** . . . (**S304–S307**). Each individual ATM cell reconstructed by the above steps is sequentially clocked out for transmission to the terminal designated by the VPI of the cell. When the transmission is completed, each block is reset to complete the receive process (**S308–S310**). Non-multiplexed cells are sent out to the designated terminals without undergoing the above process (**S311, S312**).

Next, using the functional configuration of FIG. **22** and the control flow of FIG. **23**, the operation of the demultiplexer **85** will be described below when the representative VPI (2) shown in FIG. **8** and related to FIG. **19** is used.

The configuration shown in FIG. **22** is substantially the same as that shown in FIG. **20**; in FIG. **22**, corresponding parts to those shown in FIG. **20** are designated by the same reference numerals, and therefore, descriptions of such parts are not repeated here. As described with reference to FIG. **19**, each multiplexed cell is detected by the detector **84**, and the individual VPI numbers (VPI #**121**, VPI #**122**) of the component cells are obtained from the corresponding VPI management table **83**.

The difference from the configuration of FIG. **20** is that in FIG. **22**, the VPI numbers obtained from the VPI management table **83** are written into the ATM cell areas in the respective cell buffers via the read/write circuit **95**.

In the configuration of FIG. **20** also, in cases in which VPI identifiers indicating addresses within the VPI management table are written in the information field storing area, the VPI numbers obtained from the VPI management table are written into the ATM cell areas of the respective cell buffers via the read/write circuit **95**, as in the above configuration.

FIG. **23** shows an example of a control flow for FIG. **22**.

In FIG. **23**, the GFC area (AAAA) is checked in step **S402** to detect a representative VPI. If AAAA are not all 0s, then the cell is determined as a multiplexed cell, and the received cell is written into the multiplex buffer **94** (**S403**). Next, from the addresses within the VPI management table corresponding to the AAAA, the VPI numbers stored at the addresses designated by the address flags X_0–X_7 whose value is set to "1" are extracted and written into the cell buffers as VPIs (**S404–S406**). Next, the information fields of the individual cells are read out of the information field storing area in the multiplex buffer and written into the respectively corresponding cell buffers (**S407**). The ATM cells are thus reconstructed. After that, each cell is sequentially clocked out for transmission to the terminal designated by the VPI of the cell (**S408, S410**).

FIG. **24** hereinafter described concerns an embodiment in which the input buffers **51** in the transmitting section shown in FIG. **10** are provided with a congestion prediction function.

In FIG. **24**, each input buffer **51** at the transmitting side is constructed, for example, from a first-in, first-out (FIFO) buffer memory or from a RAM, and is so configured as to output a congestion prediction signal when the number of received cells being buffered exceeds a prescribed number. For example, if the buffer has the capacity for 100 cells, the congestion prediction signal is issued when the number of buffered cells reaches **80**. Upon reception of this signal, the multiplexer **56** (FIG. **10**) starts cell multiplexing to reduce the number of cells and thereby prevent the occurrence of path congestion. The cell multiplexing is stopped upon the removal of the above signal. Such control is performed to prevent cell transmission delays when no congestion is expected.

In the above example, cell multiplex control to prevent congestion is performed within the cell multiplexing apparatus itself, but such control may be performed between communication nodes. Taking the network shown in FIG. **9** as an example, when a congestion prediction signal is issued in the ATM exchange (3) **46** by way of a common line signal, a control cell, etc., the ATM exchange (3) **46** alerts the ATM exchange (2) **43** accordingly. The alerted ATM exchange (2) **43** then starts multiplexing the cells to be transmitted onto the designated path. In like manner, the ATM exchange (2) **43** alerts the ATM exchange (1) **42** which then starts cell multiplexing in the same manner as above. As a result, the number of cells to be transmitted to the ATM exchange (3) **46** is reduced, and the occurrence of path congestion is thus prevented.

FIG. **25** shows an example in which each input buffer in the transmitting section is a FIFO buffer memory.

In FIG. **25**, if each FIFO buffer **101** has a depth for ten cells, the following FIFO flag outputs are supplied to a selector **102** at the next stage; that is, a half-flag **1** is set when the number of input cells reaches five, and a full-flag **1** is set when the number reaches 10, and likewise, a half-flag **2** and a full-flag **2** are set when the number of input cells reaches **15** and **20**, respectively. Any one of these flag outputs can be selected by setting an appropriate value in a cell count setting register **103**. By using the selected flag output as the congestion prediction signal, i.e., the multiplex start signal, cell multiplex control can be performed to match various congestion conditions.

FIG. **26** shows an example in which each input buffer in the transmitting section is constructed from a RAM.

In FIG. **26**, a read address pointer (RP) **104** and a write address pointer (WP)**105** respectively indicate RAM read/write (input/output) addresses, either one of which is selected by an address select circuit **106** for input to a RAM **107**. Read enable/write enable signals control the selection of one or other of the pointers, **104** or **105**, and switches the address select circuit **106** accordingly. The pointers **104** and **105** are each constructed from a ring counter which circulates in a cyclic manner, completing one cycle with a prescribed number of system clock pulses. A subtractor **108** obtains the difference between the addresses fed from the

read address pointer 104 and the write address pointer 105. The difference obtained by the subtractor 108 is supplied to a comparator 109 at the next stage, where the difference is compared with the set value of the cell count setting register 110. The multiplex start signal is output when the difference between the read (output) address and the write (input) address exceeds the set value.

For example, when the read address pointer indicates 035 hex and the write address pointer indicates 048B hex, then the difference is 459 hex. Since one cell consists of 53 octets, which is 35 hex in hexadecimal notation, the difference 459 hex is equivalent to 15 cells. This difference is compared with the value set in the cell count setting register 110. While this configuration makes the circuit more complex compared with that constructed with the FIFO buffers first described, the advantage is that the cell count that evokes the multiplex start signal can be set at a desired value.

As described, according to the present invention, cells having different VPIs can be multiplexed if they are intended for transmission along the same path. This serves to enhance cell utilization, and also, the resulting reduction in the number of cells is effective in preventing path congestion.

Furthermore, since the invention is targeted at the cells intended for transmission along the same path, cell multiplexing is performed only in the ATM exchange at the UNI side, and processing such as multiplexing and demultiplexing need not be performed in intermediate ATM exchanges. This serves to eliminate cell transmission delays associated with such processing, and realizes cell multiplexing that ensures almost real-time transmission.

I claim:

1. A cell multiplexing apparatus in an ATM network, comprising: transmitting means in which information fields of a plurality of ATM cells with different path identifiers intended for transmission along the same path are multiplexed and stored into an information field of one multiplexed cell, and a representative path identifier globally, representing the path identifiers of said plurality of ATM cells intended for transmission along said same path, is assigned as the path identifier of said multiplexed cell for transmission; and receiving means in which said representative path identifier is detected from received cells and said plurality of ATM cells having individual path identifiers and transmitted along said same path are reconstructed from said multiplexed cell having said representative path identifier.

2. A cell multiplexing apparatus in an ATM network according to claim 1, wherein said multiplexed cell carries said representative path identifier in an ATM header thereof, and individual path identifier information, designated by said representative path identifier, of said plurality of ATM cells intended for transmission along said same path in an information field thereof.

3. A cell multiplexing apparatus in an ATM network according to claim 1, wherein a path identifier area in an ATM header of said multiplexed cell is divided into two segments so that said representative path identifier designating the path for said multiplexed cell is carried in one segment and path identifier information of said plurality of ATM cells intended for transmission along said same path is carried in the other segment.

4. A cell multiplexing apparatus in an ATM network according to claim 3, wherein said representative path identifier is assigned to a GFC area of an ATM cell format of a user network interface, UNI, at a node-to-network interface, NNI, and the path identifier information of said plurality of ATM cells intended for transmission along said same path is assigned to representative bits in the remaining path identifier area as identifiers that individually indicate the use of a plurality of path identifiers on said same path.

5. A cell multiplexing apparatus in an ATM network according to claim 1, wherein said representative path identifier is given as an initial value permanently assigned to each individual communication node, or as a variable value that is determined in accordance with a prescribed communication protocol prior to communication with the destination node.

6. A cell multiplexing apparatus in an ATM network according to claim 2, wherein said representative path identifier is given as an initial value permanently assigned to each individual communication node, or as a variable value that is determined in accordance with a prescribed communication protocol prior to communication with the destination node.

7. A cell multiplexing apparatus in an ATM network according to claim 3, wherein said representative path identifier is given as an initial value permanently assigned to each individual communication node, or as a variable value that is determined in accordance with a prescribed communication protocol prior to communication with the destination node.

8. A cell multiplexing apparatus in an ATM network according to claim 4, wherein said representative path identifier is given as an initial value permanently assigned to each individual communication node, or as a variable value that is determined in accordance with a prescribed communication protocol prior to communication with the destination node.

9. A cell multiplexing apparatus in an ATM network according to claim 1, wherein said transmitting means includes congestion predicting means for predicting the occurrence of congestion from the relationship between the number of input cells and the number of output cells, said multiplexed cell being assembled and transmitted only when the occurrence of congestion is predicted.

10. A cell multiplexing apparatus in an ATM network, comprising transmitting means which includes: input buffer means for buffering a prescribed number of input cells; path identifier managing means for managing path identifiers of a plurality of ATM cells with different path identifiers to be transmitted along the same path; representative path identifier assigning means for assigning one representative path identifier representing the path identifiers of said plurality of ATM cells to be transmitted along said same path; path match detecting means for comparing the path identifier of each of said input cells supplied from said input buffer means with path identifiers supplied from said managing means as designating the same path, and thereby separating said input cells into matched cells and unmatched cells for output; multiplexed cell assembling means for assembling said matched input cells supplied from said path match detecting means into one multiplexed cell and for assigning said representative path identifier supplied from said representative path identifier assigning means as the path identifier of said multiplexed cell; and output buffer means for buffering said multiplexed cell from said multiplexed cell assembling means and/or said unmatched input cells from said path match detecting means for output; and

receiving means which includes: input buffer means for buffering a prescribed number of received cells; representative path identifier assigning means for assigning a representative path identifier for a multiplexed cell assembled from a plurality of ATM cells with different path identifiers to be transmitted along the same path; path identifier managing means for managing path

identifiers of said plurality of ATM cells that form said multiplexed cell; representative path identifier detecting means for comparing the path identifier of each of said received cells supplied from said input buffer means with said representative path identifier supplied from said representative path identifier assigning means, and thereby separating said received cells into multiplexed cells having a matched representative path identifier and other received cells for output; multiplexed cell disassembling means for disassembling each of said matched multiplexed cells supplied from said representative path identifier detecting means into said plurality of ATM cells forming said multiplexed cell; and output buffer means for buffering said plurality of ATM cells from said multiplexed cell disassembling means and/or said unmatched received cells from said representative path identifier detecting means for output.

11. A cell multiplexing apparatus in an ATM network according to claim 10, wherein in said path identifier managing means, said representative path identifier, which is given as an initial value permanently assigned to each individual communication node or as a set value variably determined in accordance with a prescribed communication protocol prior to communication with the destination node, and said plurality of path identifiers designated by said representative path identifier are contained in accordance with a prescribed format.

12. A cell multiplexing apparatus in an ATM network comprising transmitting means which includes: input buffer means for buffering a prescribed number of input cells; path identifier managing means for managing path identifiers of a plurality of ATM is to be transmitted along the same path; representative path identifier assigning means for assigning one representative path identifier representing the path identifiers of said plurality of ATM cells to be transmitted along said same path; path match detecting means for comparing the path identifier of each of said input cells supplied from said input buffer means with path identifiers supplied from Said managing means as designating the same path, and thereby separating said input cells into matched cells and unmatched cells for output; multiplexed cell assembling means for assembling said matched input cells supplied from said path match detecting means into one multiplexed cell and for assigning said representative path identifier supplied from said representative path identifier assigning means as the path identifier of said multiplexed cell; and output buffer means for buffering said multiplexed cell from said multiplexed cell assembling means and/or said unmatched input cells from said path match detecting means for output; and receiving means which includes: input buffer means for buffering a prescribed number of received cells; representative path identifier assigning means for assigning a representative path identifier for a multiplexed cell assembled from a plurality of ATM cells to be transmitted along the same path; path identifier managing means for managing path identifiers of said plurality of ATM cells that form said multiplexed cell; representative path identifier detecting means for comparing the path identifier of each of said received cells supplied from said input buffer means with said representative path identifier supplied from said representative path identifier assigning means, and thereby separating said received cells into multiplexed cells having a matched representative path identifier and other received cells for output; multiplexed cell disassembling means for dissasembling each of said matched multiplexed cells supplied from said representative path identifier detecting means into said plurality of ATM cells forming said multiplexed cell; and output buffer means for buffering said plurality of ATM cells from said multiplexed cell disassembling means and/or said unmatched received cells from said representative path identifier detecting means for output,

in said path identifier managing means, said representative path identifier, which is given as an initial value permanently assigned to each individual communication node or as a set value variably determined in accordance with a prescribed communication protocol prior to communication with the destination node, and said plurality of path identifiers designated by said representive path identifier, are contained in accordance with a prescribed format, and

wherein said prescribed format is comprised of: said representative path identifier set at a prescribed address; and said plurality of path identifiers for said same path, set at addresses within a prescribed range before or after said representative path identifier.

13. A cell multiplexing apparatus in an ATM network according to claim 11, wherein said prescribed format is comprised of: a memory area designated by said representative path identifier assigned to a GFC area of an ATM cell format of a user network interface, UNI, at a node-to-network interface, NNI; and said plurality of path identifier for said same path, set at memory addresses within a memory area designated by the path identifiers that are assigned to respective bits in other path identifiers areas than said GFC area as identifiers that individually indicate the use of said plurality of path identifiers on said same path.

14. A cell multiplexing apparatus in an ATM network according to claim 10, wherein said input buffer means of said transmitting means issues a congestion prediction signal when the number of input cells being buffered has reached a prescribed number, and said path identifier managing means controls said path match detecting means so that multiplexed cell assembly is started when said congestion prediction signal is issued, and is stopped when said congestion prediction signal is removed.

15. A multiplexing apparatus for multiplexing fixed length packets transmitted in a communication network, the apparatus comprising:

information multiplexing means for multiplexing information fields of a plurality of fixed-length packets with different path identifiers transmitted along the same path, so that an information field of a fixed-length packet includes the information fields of a plurality of fixed-length packets;

identifier producing means for assigning a second identifier that represents in common first identifiers assigned to said plurality of fixed length packets transmitted along the same path direction; and

fixed length packet producing means for producing a fixed length packet by adding the second identifier produced by said identifier producing means to the information field produced by said information multiplexing means.

16. A multiplexing apparatus for multiplexing fixed length packets transmitted in a common network, the apparatus comprising:

detecting means for detecting a second identifier from a fixed length packet that includes an information field relating to multiplexed information fields of a plurality of fixed-length packets with different path identifiers transmitted along the same path, and the second identifier that represents in common the first identifier assigned to said plurality of fixed-length packets transmitted along the same path direction;

separating means for separating said multiplexed information fields included in an information field of said fixed length packet together with said second identifier; and

reproducing means for reproducing said original fixed-length packets by adding said first identifier to each information field separated by said separating means.

17. An apparatus for transmitting a fixed length packet having a header and information, the apparatus comprising:

receiving means for said fixed length packet;

information multiplexing means for multiplexing the information of a plurality of said fixed-length packets with different path identifiers transmitted along the same path;

multiplexing information adding means for adding a header, together with multiplexing information indicating that information is multiplexed by said information multiplexing means, to said information multiplexed; and

transmitting means for transmitting a fixed length packet produced by said multiplexing information adding means.

18. An apparatus for transmitting a fixed length packet consisting of a header and information; the apparatus comprising:

receiving means for receiving a fixed length packet having information provided by multiplexing information of a plurality of said fixed length packets with different path identifiers transmitted along the same path, and a header together with an identifier that indicates information of a plurality of said fixed-length packets is multiplexed;

separating means for separating said multiplexed information of said fixed-length packets;

header adding means for adding a header to each information separated by said separating means; and

transmitting means for transmitting a plurality of fixed length packets produced by said header adding means.

* * * * *

US005566179A

United States Patent [19]

Kobayashi et al.

[11] Patent Number: 5,566,179

[45] Date of Patent: Oct. 15, 1996

[54] BROADBAND SWITCHING NETWORKS

[75] Inventors: Hiroshi Kobayashi, Tokyo; Toshikazu Kodama, Kanagawa-ken; Keiichi Obara, Tokyo, all of Japan

[73] Assignee: Kabushiki Kaisha Toshiba, Kanagawa-ken, Japan

[21] Appl. No.: 315,495

[22] Filed: Sep. 30, 1994

Related U.S. Application Data

[63] Continuation of Ser. No. 747,240, Aug. 19, 1991, abandoned.

[30] **Foreign Application Priority Data**

Aug. 18, 1990 [JP] Japan 2-217677

[51] Int. Cl.[6] H04J 3/00

[52] U.S. Cl. 370/85.15; 370/85.12; 370/85.13; 370/85.14; 370/94.1

[58] Field of Search 370/94.1, 60, 58.1, 370/110.1, 85.7, 85.12, 85.13, 85.14, 85.15, 60.1, 95.1

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,569,041	2/1986	Takeuchi et al.	370/85.12
4,663,748	5/1987	Karbowiak et al.	370/85.12
4,875,206	10/1989	Nichols et al.	370/85.15
4,947,390	8/1990	Sheehy	370/85.13
4,955,019	9/1990	Mizuhara et al.	370/85.7
5,130,984	7/1992	Cisneros	370/94.1
5,134,612	7/1992	Yoshimura	370/84
5,187,706	2/1993	Frankel et al.	370/85.14
5,214,648	5/1993	Lespagnol et al.	370/94.1
5,280,475	1/1994	Yanagi et al.	370/60
5,282,207	1/1994	Jurkevich et al.	370/94.1
5,289,462	2/1994	Ahmadi et al.	370/79

FOREIGN PATENT DOCUMENTS

0119105	9/1984	European Pat. Off. .
2-195751	8/1990	Japan .

OTHER PUBLICATIONS

E. Matthias et al., "Strategy for an ATM Interconnect Network", Proceedings International Switching Symposium, vol. 4, May 28 through Jun. 1, 1990, pp. 29–33.

H. Yamashita et al., "Flexible Synchronous Broad-Band Subscriber Loop System: Optical Shuttle Bus", IEEE Journal of Lightwave Technology, vol. 7, No. 11, Nov. 1989, pp. 1788–1797.

S. J. Golestani, "Congestion-Free Communication in Broadband Packet Networks", IEEE International Conference on Communications, vol. 2, Apr. 15–19, 1990, pp. 489–494.

"Recommendations Drafted by Working Party XVIII/8 (General B-ISDN Aspects) to be Approved in 1990" by the Study Group XVIII (Geneva Meeting, 23–25 May 1990), CCITT Report R 34.

Feng 'A Survey of Interconnection Networks' IEEE Computer, 1981, Dec. 12–27.

Primary Examiner—Douglas W. Olms
Assistant Examiner—Shick Hom
Attorney, Agent, or Firm—Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P.

[57] **ABSTRACT**

A broadband switching network for transmitting information by using a cell composed of an information field and a header, including a first network comprising an ATM ring having a plurality of access nodes for multiplexing and demultiplexing the cell and a ring shape transmission path for connecting the plurality of access nodes in a ring shape so as to transmit the cell, and at least one second network, wherein the first network being connected to at least one second network via one of the plurality of access nodes, each second network having a switching function for switching the cell.

16 Claims, 8 Drawing Sheets

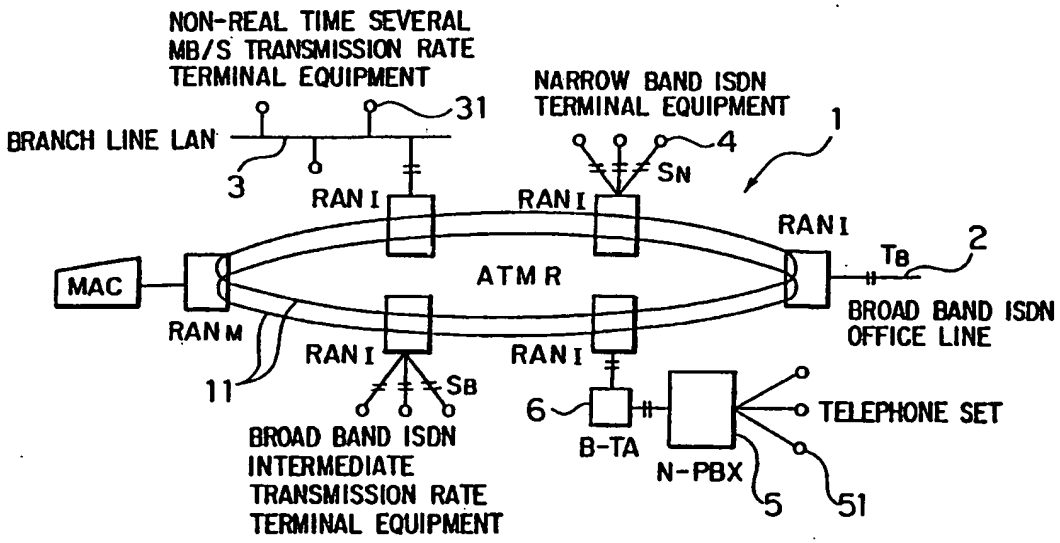


FIG. 1

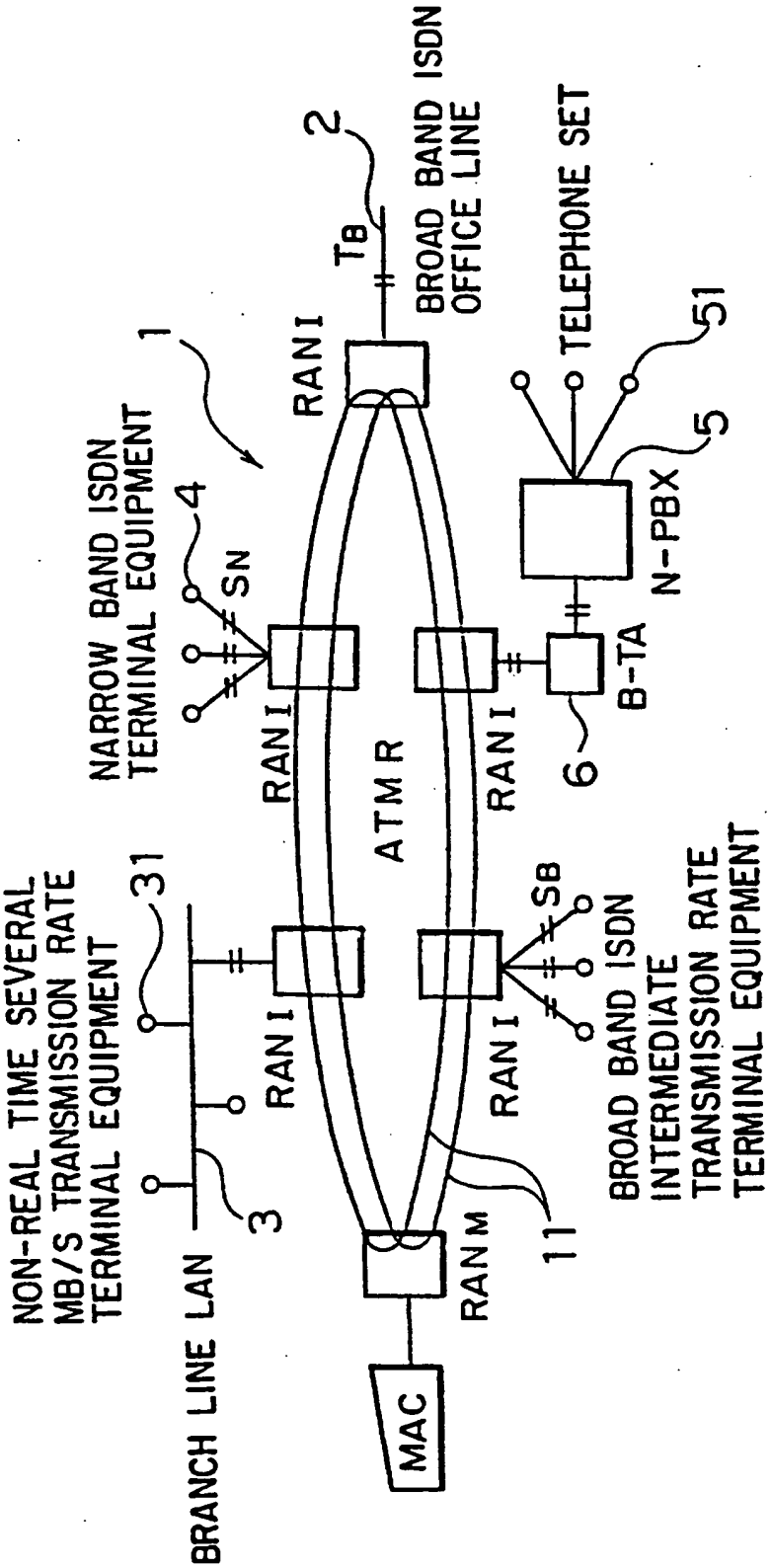

NON-REAL TIME SEVERAL MB/S TRANSMISSION RATE TERMINAL EQUIPMENT
31
BRANCH LINE LAN
3
NARROW BAND ISDN TERMINAL EQUIPMENT
4
SN
1
RAN I
RAN I
ATM R
RAN I
RAN I
RAN M
MAC
11
TB
2
BROAD BAND ISDN OFFICE LINE
SB
BROAD BAND ISDN INTERMEDIATE TRANSMISSION RATE TERMINAL EQUIPMENT
TELEPHONE SET
51
5
N-PBX
B-TA
6

FIG. 2

CHARACTERISTICS AND RATIOS OF TYPES OF TERMINAL EQUIPMENTS

TERMINAL TYPE	ALL SERVICE TYPE CATEGORY	MAXIMUM TRANSMISSION RATE (MB/S)	AVERAGE TRANSMISSION RATE (MB/S)	ASYMMETRICAL COEFFICIENT	RATIOS OF TYPES OF TERMINAL EQUIPMENTS (%)
① NARROW BAND ISDN TERMINAL EQUIPMENT (STM TERMINAL EQUIPMENT)	1	0.09	0.09	1.00	45.4
② NON-REAL TIME SEVERAL MB/S TRANSMISSION RATE TERMINAL EQUIPMENT	3 / 4	2.20	0.60	0.61	39.0
③ REAL TIME SEVERAL MB/S TRANSMISSION RATE TERMINAL EQUIPMENT	2	1.83	0.74	0.59	6.5
④ BROAD BAND ISDN INTERMEDIATE TERMINAL EQUIPMENT (H2)	2	40.00	11.78	0.50	9.1
⑤ BROAD BAND ISDN HIGH TRANSMISSION RATE TERMINAL EQUIPMENT (H4)	B	145	106	0:50	FEW

FIG. 3

OUTLINE AND EXAMPLE OF CONSTRUCTION OF SYSTEM ARCHITECTURE

		SMALL CAPACITY SYSTEM	INTERMEDIATE CAPACITY SYSTEM	LARGE CAPACITY SYSTEM	
NUMBER OF TERMINAL EQUIPMENT INTERFACES		~400	~1600	~6000	~16000
NUMBER OF ATMR'S		1	-4	-15	-40
NUMBER OF ATMR'S		—	1	-6	-8
ATMT SWITCH SIZE		—	16 × 16	16 × 16	32 × 32
ATMR CALL PROCESS CAPACITY (BHCA)		≧5400	≧7200	≧7200	≧7200
ATMT CALL PROCESS CAPACITY (BHCA)		—	≧28800	≧28800	≧43200
STAGE REQUIRED	INTRODUCTION STAGE	○			
	DEVELOPMENT STAGE	○	○		
	POPULARIZATION STAGE	○	○	○	○

FIG. 4

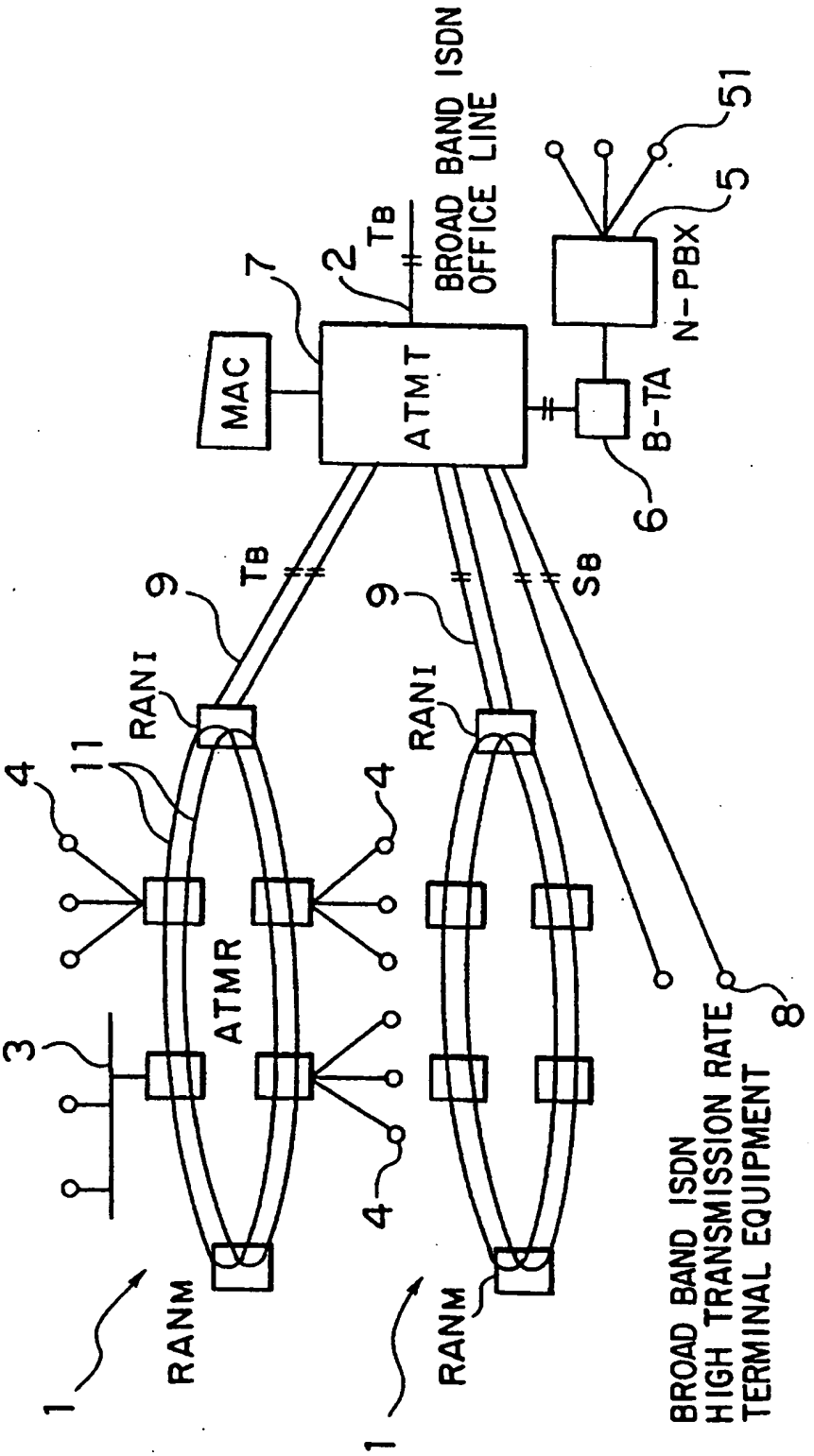

BROAD BAND ISDN
OFFICE LINE
TB
2
7
MAC
ATMT
B-TA
6
N-PBX
5
51
TB
SB
9
9
RANI
RANI
11
4
4
4
4
ATMR
3
RANM
RANM
1
1
BROAD BAND ISDN
HIGH TRANSMISSION RATE
TERMINAL EQUIPMENT
8

FIG. 5

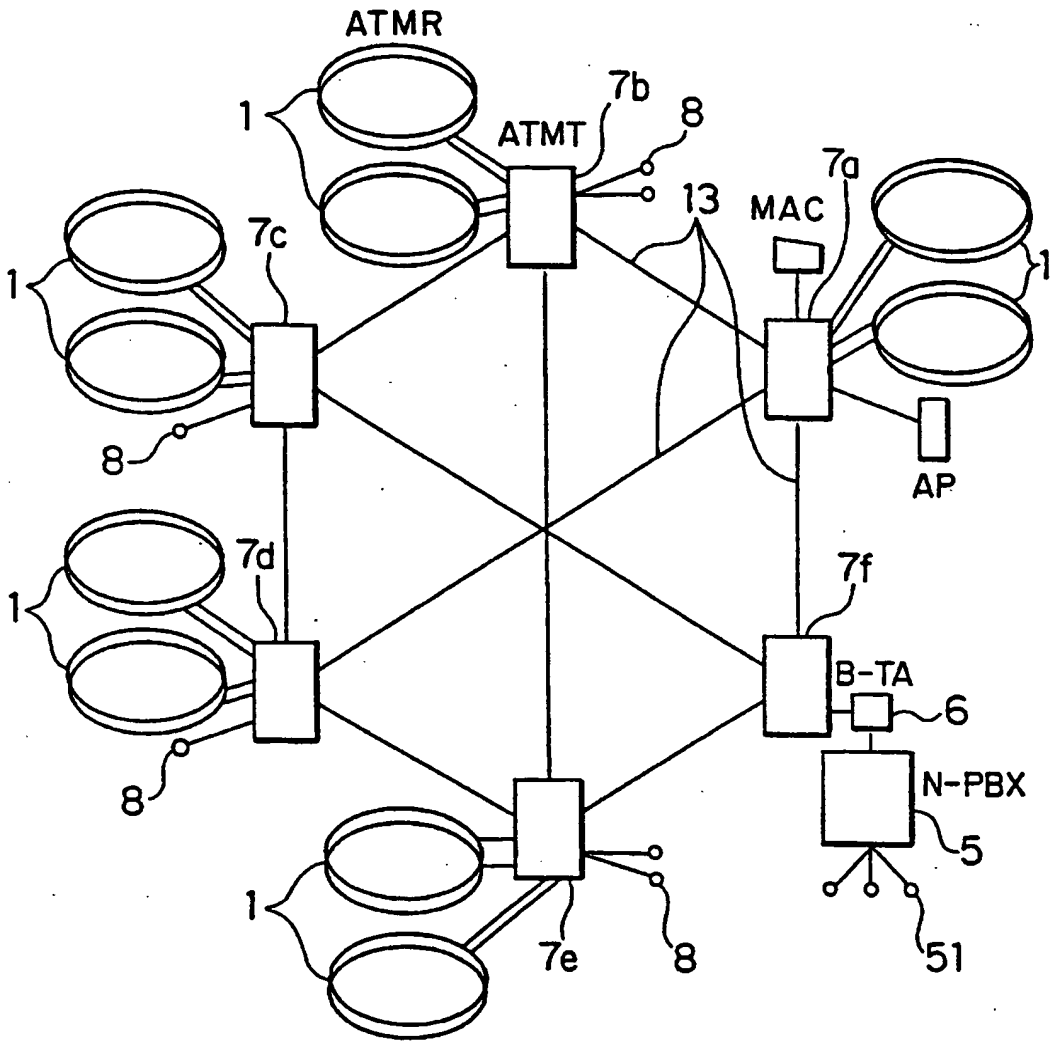


FIG. 6

LOOP NETWORK CONNECTION

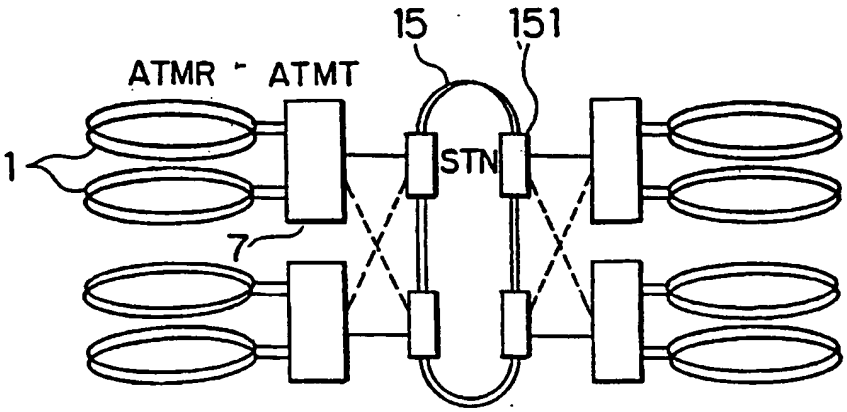


FIG. 7

WHEEL SHAPE CONNECTION

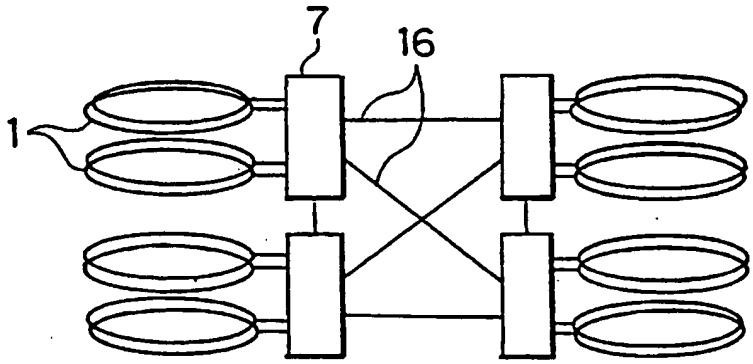


FIG. 8

RING SHAPE CONNECTION

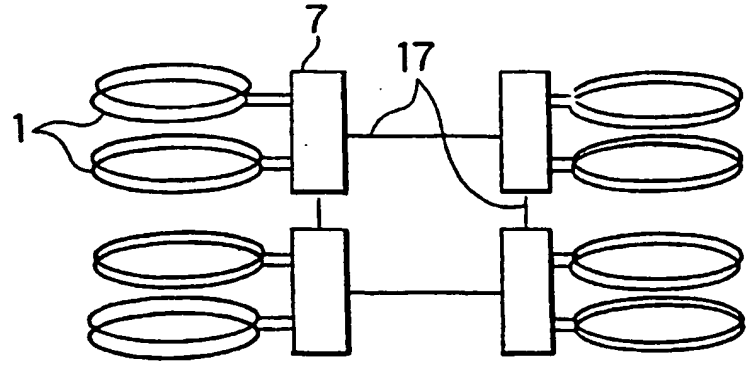


FIG. 9

COMPARISON OF CONNECTION METHODS AMONG ATMT'S

NUMBER OF TERMINAL EQUIPMENT INTERFACES	4000 TERMINAL EQUIPMENT INTERFACES			6000 TERMINAL EQUIPMENT INTERFACES			16000 TERMINAL EQUIPMENT INTERFACES		
CONNECTION METHOD	LOOP	WHEEL SHAPE	RING SHAPE	LOOP	WHEEL SHAPE	RING SHAPE	LOOP	WHEEL SHAPE	RING SHAPE
NUMBER OF ATMR SYSTEMS	10			15			40		
NUMBER OF ATMT PORTS	16			16		32	16	32	64
NUMBER OF ATMT'S	4			6		3	16	8	4
NUMBER OF ATMR CONNECTION PORTS	5			5		10	5	10	20
NUMBER OF ATMT CONNECTION PORTS	4	6	6	5	6	8	5	14	22
NUMBER OF OFFICE LINE CONNECTION PORTS	3			3		5	3	5	10
ATMT PORT UTILIZATION EFFICIENCY	12/16	14/16	14/16	13/16	14/16	23/32	13/16	29/32	52/64
LOOP TRANSMISSION RATE (Gb/s)	2.3	—		3.3	—		8.0	—	

FIG. 10

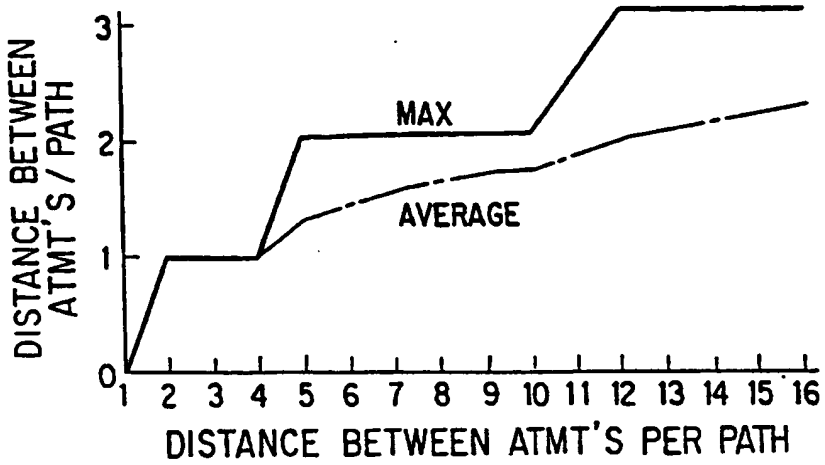


FIG. 11

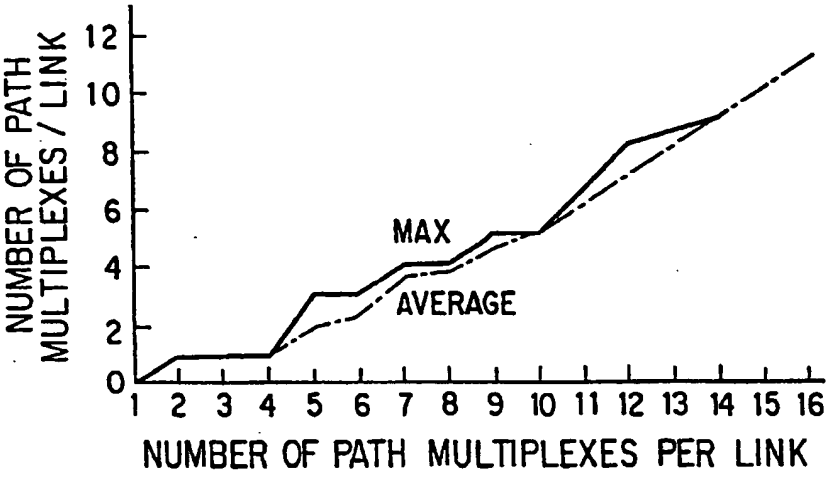
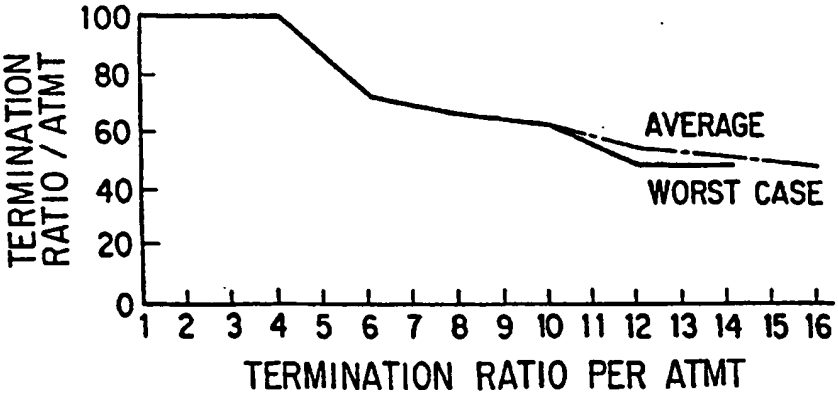


FIG. 12



BROADBAND SWITCHING NETWORKS

This application is a continuation of application Ser. No. 07/747,240, filed Aug. 19, 1991, now abandoned.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to broadband switching networks based on a broadband ISDN using ATM (Asynchronous Transfer Mode) technologies for use in companies.

2. Description of the Related Art

Efforts for integrating individual service networks such as telephone networks, data networks, FAX networks, and so forth which have been developed and constructed over 100 years of history into one network system with ISDN (Integrated Services Digital Network) have been made throughout the world.

As the first step for constructing the ISDN system, narrow band ISDN systems have been operated in advanced countries including Japan since 1988. In addition, besides integration with a broadcasting network by using a broadband ISDN based on the ATM technologies, the engineering developments of the ISDN network have been initiated by CCITT (International Telegraph and Telephone Consultative Committee) and promoted in major laboratories in the world.

On the way of introduction, development, and popularization of the broadband ISDN for use in companies, it can be estimated that small capacity systems on the order of several ten of terminal equipments to several hundreds of terminal equipments as initial installations will be expanded to large capacity systems of for example 16000 terminal equipment.

Thus, from the standpoint of cost required for the expansion, a consistent architecture is preferable for the broadband switching network for use in companies.

However, thus far, a broadband switching network with a consistent architecture has not been proposed. Thereby, the broadband ISDN for use in companies has not been satisfactorily introduced.

As was described above, since the architecture of the systems has not been consistent in the introduction stage, the development stage, and the popularization stage, equipment which has been introduced cannot be effectively used for expanding the systems and thereby result in many losses.

SUMMARY OF THE INVENTION

An object of the present invention is to solve such a problem and to provide broadband switching networks which can be constructed with the same architecture as that from small capacity systems to large capacity systems.

To accomplish the above mentioned object, the broadband switching network according to the present invention is a broadband switching network for transmitting information by using a cell composed of an information field and a header, the network comprising a first network having a plurality of access nodes for multiplexing and demultiplexing the cell and a ring shape transmission path for connecting the plurality of access nodes in a ring shape so as to transmit the cell, and a second network connected to at least one of the plurality of access nodes, the second network having a switching function for relaying and switching the cell.

In addition, by any combination of the broadband switching node and the first network connected therewith, the system can be expanded from a small capacity system into a large capacity system with the same architecture.

BRIEF DESCRIPTION OF DRAWINGS

FIG. 1 is a schematic showing a construction of a small capacity system of a broadband switching system according to an embodiment of the present invention;

FIG. 2 is a table showing an example of characteristics and ratios of various terminal equipments connected to a broadband switching network;

FIG. 3 is a table showing an outline of system architectures;

FIG. 4 is a schematic showing a construction of an intermediate capacity system of the broadband switching network according to the embodiment of the present invention;

FIG. 5 is a schematic showing a construction of a large capacity system of the broadband switching network according to the embodiment of the present invention;

FIG. 6 is a schematic showing a construction of ATMTs mutually connected with a loop network linkage;

FIG. 7 is a schematic showing a construction of ATMTs mutually connected with a wheel shape linkage;

FIG. 8 is a schematic showing a construction of ATMTs mutually connected with a ring shape linkage;

FIG. 9 is a table showing examples of constructions of broadband switching networks by the number of terminal equipment interfaces and by methods mutually connected among ATMTs;

FIG. 10 is a diagram showing the relation between the distance between ATMTs per path and the number of ATMTs;

FIG. 11 is a diagram showing the relation between the number of path multiplexes per link and the number of ATMTs; and

FIG. 12 is a diagram showing the relation between the termination ratio per ATMT and the number of ATMTs.

DESCRIPTION OF PREFERRED EMBODIMENTS

With reference to the accompanying drawings, an embodiment of the present invention will be described. The same portions of each drawing use the same reference numerals. The description of overlapped portions is omitted.

SMALL CAPACITY SYSTEMS

FIG. 1 is a schematic showing a construction of a small capacity system of a broadband switching network according to an embodiment of the present invention.

In the figure, reference numeral 1 is an ATM ring (hereinafter named the ATMR).

The ATMR 1 is composed of two types of ring access nodes (hereinafter named the RANs), a maintenance console (hereinafter named the MAC), and two systems of optical rings 11.

The RAN is provided with a terminal equipment interface accommodating ring access node (hereinafter named the RAN_t) for accommodating various terminal equipment interfaces, an office line interface, and so forth; and a call process management ring access node RAN_M for perform-

ing the call process, the maintenance, and the management of the entire ATMR 1.

The ATMR 1 is connected to a broadband ISDN office line 2 through one of RAN_Bs. In addition, the RAN_I is connected for example to a bronch line LAN (Local Area Network) 3, which is connected with non-real time several Mb/s transmission rate terminal equipments 31; narrow band ISDN terminal equipments 4; an STM base PBX (N-PBX) 5; broadband ISDN intermediate transmission rate terminal equipments 6; and so forth. The N-PBX 5 is connected with non-ISDN terminal equipments 51. The narrowband ISDN PBX 5 is connected to the RAN_I through a terminal adapter (B-TA) 6.

The ATMR 1 in the above mentioned construction can operate autonomously without a connection with a distributed switch tandem node (hereinafter named the ATMT). Thus, small capacity systems in the range from several terminal equipments to several hundred terminal equipments can be inexpensively constructed.

The RAN_I can accommodate for example six lines of LAN interfaces, six lines of S_B interfaces, eight lines of narrow band ISDN interfaces, one line of 1.5 Mb/s primary group interface, one line of 6.3 Mb/s high transmission rate digital line interface, or the like depending on the selection of a terminal equipment interface card thereof.

In particular, the RAN_I which accommodates an interface card that connects an office line or an ATMT (not shown in the figure) is provided with functions for supplying a clock to the ATMR 1 and for monitoring it and a traffic shaping function for suppressing the burstiness of cell flow and so forth.

For example, the traffic shaping function may be realized as described in "Recommendations Drafted by Working Party XVIII/8 (General B-ISDN Aspects) to be Approved in 1990" by the Study Group XVIII (Geneva Meeting, 23–25 May 1990), CCITT Report R 34.

In the above conventional device, a buffer is provided in RAN_Is as an interface to the broadband ISDN office line 2. When a flow of cells concentrates on a broadband ISDN office line 2, the buffer stores the cells and each cell stored in the buffer flows into the broadband ISDN office line 2 with a determined delay time.

In addition, the ATMR 1 can accommodate up to 63 RANs. In particular, the RAN_M, can be duplexed. Even if the power of the MAC is turned off, the ATMR can be continuously operated. By connecting a plurality of MACs to the RAN_M, they can be used for dedicated functions such as data setting, status display, charging process, and traffic calculation.

In FIG. 1, the STM base N-PBX 5 can interwork with the broadband switching network through the primary group interface (H11) and thereby mutually communicate with narrow ISDN telephone terminal equipments in the system, and access the broadband ISDN network. In addition, with an ATM cell through a multiplex interface such as the above mentioned primary group interface or a TTC 2M standard interface in the circuit emulation method, a dedicated line on the broadband ISDN base can communicate with an N-PBX at a distant location through a broadband switching network thereof. Thus, since the broadband ISDN dedicated line is shared with another broadband traffic, the communication cost can be decreased.

The number of terminal equipment interfaces that the ATMR 1 can accommodate is determined by the limitation of the traffic peak load ratio. The traffic peak load ratio is a ratio of the sum of the maximum transmission rate that the user declares before making a communication (or the average transmission rate for a call which does not require a real time communication) and the payload capacity. In other words, the RAN_I which is connected to an office line with the heaviest load should satisfy the following equation.

$$N \times \eta \times (Ct+Ce) \times Sp \times \alpha \leq Tp \times \psi p \times \epsilon \times R \quad (1)$$

where $Sp=\Sigma (Si \times Ni \times Bi)$ (=2.07 Mb/s, from FIG. 2);

N: Number of terminal equipment interfaces which can be accommodated

η=0.3: Ratio of terminal equipments which are used in the maximum load state

Ct=1.0: Ratio of bidirectional connections of office line

Ce=0.5: Ratio of bidirectional connections of extension

α: Safety ratio

Tp=149.76 Mb/s: Payload capacity

ψp=95%: Traffic peak ratio

ϵ=2.0: Average reuse ratio of cells

R=2: Number of rings

Si: Maximum/average transmission rate of terminal equipment (Average transmission rate for non-real time several Mb/s transmission rate terminal equipment)

Bi: Asymmetrical coefficient

Ni: Ratio of terminal equipments

The average reuse ratio of cells, ϵ, which is intrinsic to the ATMR is in the range from 1 to 4 depending on the traffic distribution therein. However, in consideration of concentration of the traffic to the RAN_I which accommodates the office line, in this embodiment, the average reuse ratio of cells ϵ is set to 2.0.

FIG. 2 is a table showing an example of the terminal equipment maximum/average transmission rate, the asymmetrical coefficient, and the ratio of terminal equipments.

If the safety ratio is not considered in the equation (1), the number of terminal equipment interfaces which can be accommodated, N, is 609 or less.

In addition, when N is 400, the safety ratio, α, becomes 1.5 or less.

Thus, in consideration of a margin to a call loss of high transmission rate terminal equipments such as broadband ISDN intermediate terminal equipments and a consistency to intermediate or large capacity systems, the upper limit of the number of terminal equipment interfaces which can be accommodated preferably becomes approximately 400. When one of optical rings 11 stops due to a fault and thereby the system is operated as a single system, if N is approximately 400, the traffic amount exceeds the upper limit of which the one optical ring 11 can transmit data. Thus, in this case, all connections which are currently communicating cannot be accommodated. To prevent this, when the number of terminal equipment interfaces that the ATMR 1 accommodates is decreased to approximately 200 and the ATMR 1 is operated with the traffic amount which is half the maximum transmission capacity thereof, thus, even if such a fault takes place, all the connections can be accommodated. Even if the number of terminal equipments accommodated in one system of the ATMR 1 is decreased, although the cost of the RAN_I which accommodates the RAN_M and the office line is increased, the cost per terminal interface is not remarkably increased.

In addition, when the ATMR 1 accommodates 400 terminal equipments and one line of the 155 Mb/s transmission rate broadband ISDN office line (including a dedicated line service) is provided, the traffic peak load ratio, ψp, over the office line can be expressed by the following equation (2)

and thereby ψp becomes 0.83 and the safety ratio (margin), α, becomes 1.14.

$$\psi p \leq (N \times \eta \times \alpha \times Ce \times Sp) / (Tp \times L) \quad (2)$$

where N=400

L=2: Number of transmission paths (reception and transmission)

Thus, it is found that one line of the 155 Mb/s T_B interface per one system of ATMR can satisfy the above mentioned conditions.

In addition, as shown in FIG. 3, in consideration of the interwork with the same scale N-PBX (400 lines), the call process capacity of the ATMR 1 is preferably 5400 BHCA (incompleteness ratio=1.5) or more.

INTERMEDIATE CAPACITY SYSTEMS

Now an example of an intermediate capacity system according to the present invention will be described.

FIG. 4 is a schematic showing a construction of an intermediate capacity system of the broadband switching network according to the embodiment of the present invention.

In the figure, reference numeral 1 is an ATMR and reference numeral 7 is an ATMT.

The ATMT 7 is connected with a plurality of systems of ATMRs 1, a broadband ISDN office line 2, an N-PBX 5, and broadband ISDN high transmission rate terminals 8. One ATMT 7 connects the plurality of systems of the ATMRs 1 in a star shape. In addition, the ATMT 7 is connected with a MAC.

The ATMT 7 is provided with an ATM switch having 16 ports (not shown in the figure). The ATMT 7 accommodates up to four systems of ATMRs 1 through a 155 Mb/s or 622 Mb/s T_B interface 9. In addition, the office line interface is accommodated in the ATMT 7 so as to share the office line interface by the plurality of systems of the ATMRs 1.

The ATMR 1 is composed of two types of ring access nodes RAN_M and RAN_I which are connected with two systems of optical rings 11.

A common channel signaling system in accordance with the inter-PBX protocol is applied between the ATMR 1 and the ATMT 7. Thereby, advanced services such as transfer services, free numbering services, and tenant services are achieved. In addition, the ATMT 7 can accommodate an ATMR of another vendor. Moreover, multi-vendor property such as a mutual connection between other vendor products can be obtained.

In addition, the MAC connected to the ATMT 7 integratedly maintains, operates, and manages the entire system by closely connecting the ATMR 1 and the ATMT 7 with for example an internal protocol based on the NNI (Network Node Interface).

In addition, when the ATMT 7 is equipped with the interwork function with the N-PBX 5, the concentration of call amount to the ATMR 1 can be prevented.

Since the ATMT 7 is in port free construction, it can flexibly deal with the accommodation of the ATMR 1, the connection of the broadband ISDN office line, and the connection of the broadband ISDN high transmission rate terminal equipment.

In addition, by connecting the ATMR 1 and the ATMT 7 with application processors (AP), a multimedia information and a communication network which operates in conjunction with an information processing system and which provides advanced but delicate functions along with high expansibility and flexibility can be constructed.

Moreover, the ATMT 7 preferentially retrieves and/or selects a clock from a broadband ISDN network (through an office line, a dedicated line, or the like) and then supplies it to the ATMR 1. When the clock is stopped due to a fault, the ATMT 7 autonomously operates with an internal clock thereof and thereby continuing an extension system service.

The maximum number of terminal equipment interfaces N that one system of the ATMR can accommodate is approximately 400. In total, four systems of the ATMRs (with eight ports for connections of ATMRs and four ports for connections of office line connections) can be mutually connected and thereby up to 1600 terminal equipment interfaces can be accommodated.

When it is assumed that the maximum number of terminal equipment interfaces (N=400) are accommodated and all the connections in the ATMR 1 are made through the ATMT 7 between the ATMRs 1 and an ATMR of another system or a broadband ISDN office line 2, then the traffic peak load ratio ψp over the T_B interface 9 between the ATMR 1 and the ATMT 7 is expressed by the following equation (3) and thereby ψp becomes 0.83 and the safety ratio, α, becomes 1.14.

$$\psi p \leq (N \times \eta \times \alpha \times (Ct+Ce) \times Sp) / (Tp \times L \times M) \quad (3)$$

where

$Sp = \Sigma(Si \times Ni \times Bi)$ (=2.07 Mb/s, from FIG. 2)

accommodate

η=0.3: Ratio of terminal equipment which are used in the maximum load state

Ct: Ratio of bidirectional connections of office line

Ce: Ratio of bidirectional connections of extension;

$Ct=Ce=1$ (There is no closed connection in the ATMR 1.)

Tp=147.76 Mb/s: Payload capacity

∈=2.0: Average reuse ratio of cells

R=2: Number of rings

Si: Maximum/average transmission rate of terminal equipment (Average transmission rate for non-real time several Mb/s transmission rate of terminal equipment)

Bi: Asymmetrical coefficient

Ni: Ratio of terminal equipments

L=2: Number of transmission paths (reception and transmission).

M=2: Number of T_B (155 Mb/s) interfaces between ATMR 1 and ATMT 7.

In other words, it is necessary to assign one line of the 155 Mb/s T_B interface per ring or half the band of the 622 Mb/s T_B interface per system of the ATMR. Moreover, in the same condition, since the traffic peak load ratio in the ATMR 1 becomes 0.83, the matching property between the ATMR 1 and the ATMT 7 becomes high.

In addition, as was described in the section of the small capacity systems, when a fault takes place in the ATMR 1, in order to relieve all connections, the number of terminal equipment interfaces per system of ATMR should be limited to 200 or less. In this case, it is possible to provide one line of the 155 Mb/s T_B interface between the ATMR 1 and the ATMT 7. Although the cost slightly increases because of necessity of two RANm', the number of terminal equipment

interfaces which can be accommodated as the system is not changed.

In addition, the traffic peak load ratio over the broadband ISDN office line 2 per system of the ATMR is equal to the value obtained in the above mentioned equation (2). Thus, the ATMT 7 should accommodate up to four lines of the 155 Mb/s T_B interfaces or one line of the 622 Mb/s T_B interface.

In addition, the broadband ISDN high transmission rate terminal equipment 8 is directly connected to the ATMT 7 through an S_B interface. In the maximum construction where four systems of the ATMRs 1 are connected, as was described above, since 12 of 16 ports of the ATM switch resources of the ATMT 7 are used, four ports are assigned to the broadband ISDN high transmission rate terminal equipment 8. In addition, for a user who uses many connections of the broad band ISDN high transmission rate terminal equipments at the same time, the number of connections of the ATMRs 1 is limited. As another method, a plurality of ATMTs 7 are mutually connected. As another method, an ATMT with 32 ports can be used.

In addition, in the maximum construction where four systems of the ATMRs 1 are connected, as shown in FIG. 3, the call process capacity of the ATMT 7 including the interface with the same scale N-PBX (1600 lines) should be 28800 BHCA (incompleteness ratio is 1.5) or more. When all the connections in the ATMR 1 are made through the ATMT 7, the call process capacity of the ATMR 1 should be 7200 BHCA or more.

LARGE CAPACITY SYSTEMS

Then, an example of a large capacity system necessary in the popularization stage for use in companies will be described.

FIG. 5 is a schematic showing a construction of a large capacity system of the broadband switching network according to the embodiment of the present invention.

In the figure, reference numeral 1 is an ATMR which can accommodate up to 400 terminal equipments and reference numerals *7a* to *7f* are ATMTs with 16 ports.

The ATMTs *7a* to *7f* are circumferentially disposed. Regularly, any ATMT 7 is connected with another ATMT 7 through a three-way transmission path (link) 13 in a wheel shape. In addition, any ATMT 7 is connected to a broadband ISDN office line (not shown in the figure) with three ports.

Each of ATMTs *7a* to *7e* is connected to two systems of ATMRs 1.

In addition, the ATMT *7a* is connected with an MAC and an application processor (AP). On the other hand, the ATMT *7f* is connected with an N-PBX 5 through a B-TA 6.

In the construction shown in FIG. 5, up to 4000 terminal equipment interfaces are accommodated. Each of ATMTs *7a* to *7e* is connected with three systems of ATMRs 1. The entire system can accommodate 6000 terminal equipment interfaces with connections of 15 systems of ATMRs 1. In addition, the above system can be constructed with three ATMTs with 32 ports. Moreover, as an ultra large capacity system, a system which accommodates 16000 terminal equipment interfaces can be accomplished by using eight 32-port ATMTs with connections of 40 systems of ATMRs 1.

When the 16000 terminal equipment interfaces are accommodated by using eight 32-port ATMTs, each ATMT should have 10 ports for connections with the ATMR 1, five ports for connections with the office line, and 14 ports for connections with a link between the ATMTs.

In other words, since the traffic peak load ratio ψp at each port or in the ATMR 1 distributes in the range from 0.78 to 0.89 (the safety ratio is in the range from 1.07 to 1.22), the resources in the system can be almost equally used with high efficiency.

When the ATMR 1 is operated at a high transmission rate (622 Mb/s) and the capacity of the ATMT 7 is increased (with 64 ports or 128 ports), the traffic transmission capacity can be quadrupled in the same architecture without tradeoffs of the equality of services, the consistency of cost performance and reliability, the accomplishments of excellent flexibility/expansibility and standardization/multi-vendor property, and the unification of system maintenance and management.

Now another construction of mutual connections between the ATMTs 7 will be described.

FIG. 6 is a schematic showing an example of mutual connections among the ATMTs 7 with an ultra high transmission rate optical loop network 15. As shown in the figure, the ATMTs 7 are connected with stations (STNs) 151 over the optical loop network 15. In addition, the ATMTs 7 are mutually connected with other ATMTs 7 over the optical loop networks 15.

In the construction shown in FIG. 6, since signals flow in one direction. Thus, the routing control among the ATMTs 7 can be simplified. In addition, even with only one type of ATMTs, wide applications can be covered.

Against a fault, for example a dual homing system is used. In this construction, each ATMT 7 is connected with two STNs 151. When a fault takes place on the homing side STN 151 (in other words, the STN 151 to and from which the ATMT 7 transmits and receives signals), the homing side is switched to another STN 151. In addition, the optical network 15 can be also duplexed. Moreover, fault countermeasures such as loop-back or bypass against disconnection of the defective STN can be performed.

FIG. 7 is a schematic showing the construction of the system shown in FIG. 5. The ATMTs 7 are connected with three-way transmission paths (links) 16 in a wheel shape. This construction distributes the traffic into the entire system.

In this construction, as was described above, approximately up to eight ATMTs 7 can be mutually connected. The ATMTs can be linked with a standard interface transmission rate of 155 Mb/s or 622 Mb/s.

Against a fault, an advanced routing control is performed over redundant paths mutually connected from one ATMT to other three ATMTs.

FIG. 8 is a schematic showing an example of a construction where the ATMTs (links) 7 are connected in a ring shape. In this construction, the routing control of the loop network can be simplified and the link among the ATMTs 7 of the wheel shape network can be accomplished at a standard interface transmission rate.

Against a fault of one ATMT or the link among the ATMTs, the routing control is performed like the wheel shape network.

FIG. 9 is a table showing the comparison of the loop network linkage, the wheel shape network, and the ring shape network for accommodating 4000, 6000, and 16000 terminal equipment interfaces. In this table, it is assumed that the traffic peak load ratio is 90% or less.

As shown in the figure, in any construction, up to 4000 terminal equipment interfaces can be accommodated by using four ATMTs with 16-port ATM switches. The number

of ports used for data transmission among the ATMTs is four ports for the loop network linkage, and six ports for each of the wheel shape network and the ring shape network. When the ports for connections with the ATMRs and the office line are added, the number of ports for the loop network linkage is 12 ports and that for each of the wheel shape network and the ring shape network is 14 ports. The number of ports for the loop network linkage is two ports smaller than those for other methods. However, the former method has to use a 2.3 Gb/s optical loop network. The two or four ports which are not used can accommodate broadband ISDN high transmission rate terminal equipments and/or N-PBXs.

When the 6000 terminal equipment interfaces are accommodated, the loop network linkage and the wheel shape network can be constructed by using six ATMTs with 16-port ATM switches. However, the ring shape network can be constructed by using three ATMTs with 32-port ATM switches. In other words, for the ring shape network, the number of ports in use for data transmission among the ATMTs is increased. In addition, for the loop network linkage, a 3.3 Gb/s optical loop network is required.

When the 16000 terminal equipment interfaces are accommodated in the loop network linkage, 16 ATMTs with 16 ports and an 8 Gb/s optical loop network are used; in the wheel shape network, eight ATMTs with 32 ports are used; and in the ring shape network, four ATMTs with 64 ports are used.

FIGS. 10, 11, and 12 are diagrams showing the distance between the ATMTs per path, the number of path multiplexes, and the termination ratio in a non-hierarchical network construction where the distance between the ATMTs is minimum and the traffic is distributed over the entire system (for example, a wheel shape network is used when the number of ATMTs is 10 or less; a double ring shape network is used when the number of ATMTs is 11 or more) on the assumption that the direction of the traffic is at random and that the ATMTs are normally connected with three ways.

As shown in FIG. 11, the maximum number of path multiplexes is nearly equal to the average number of path multiplexes. Thus, it is found that the traffic is almost equally distributed over the network as the above mentioned first feature. In addition, as shown in FIG. 12, the worst case value of the termination ratio is almost equal to the average value of the termination ratio.

As shown in FIGS. 10, 11, and 12, when the number of ATMTs is 11 or more, the distance between ATMTs becomes 3 or more; the number of path multiplexes becomes 5 or more; and the termination ratio becomes 50% or less. In other words, 50% or more of the switching resources of the ATMTs are used only for relaying with other ATMTs. On the other hand, when the number of ATMTs is 10 or less, it is possible to keep the termination ratio 60% or more. Furthermore, in the same network construction, it is possible to increase and decrease the number of the ATMTs. In other words, when one ATMT is expansively increased, it is necessary to disconnect up to two ATMT links and then to add new three links.

In addition, as shown in FIG. 11, when a system is constructed with eight ATMTs, the number of path multiplexes per link becomes up to 4. In other words, since the number of paths routed from one ATMT to other ATMTs is 7, the 4/7 of the entire traffic flows in the link. Thus, the large capacity system which accommodates the 16000 terminal equipment interfaces can be constructed with around one line of transmission path with a transmission rate of 622 Mb/s at the link among the ATMTs rather than using an expensive, high transmission rate transmission path of Gb/s class.

In addition, since redundant links are routed among the ATMTs, a temporary deviation of the traffic can be solved with a flexible routing control without need for of special trouble countermeasures such as the switching of the homing side against the fault. Thus, it is possible to construct a system with strong resistance against the traffic deviation.

As was described above, the preferable number of the ATMTs for the wheel shape network is eight in consideration of an allowance for 2 ATMTs so as to provide flexibility and expandability after installation.

The optical fibers connected among the ATMTs are routed in a wheel shape. However, when a multiple-wire cable is routed in one stroke shape along the ATMTs, the routing work can be simplified.

In the above description, it was assumed that the traffic was almost equally distributed over the entire network. However, due to restrictions over real routing or the like, the office line may be concentratedly accommodated in one ATMT and thereby the traffic may deviate. In this case, when the connection shape among the ATMTs on the basis of wheel shape linkage, the link band (the number of ports assigned), and the capacity of the ATMTs can be properly selected, the deviation of the traffic can be solved with high flexibility. In other words, in the wheel shape network, only the connection interface between the ATMR and the ATMT restricts the flow of the traffic. Thus, the deviation of the traffic with respect to the centralized accommodation of the office line can be solved with high flexibility.

Next, the aspects of the wheel shape network composed of approximately eight ATMTs will be summarized.

First, when the direction of the traffic is random, the traffic over the network can be equally distributed without deviation to a particular link. Second, the number of links which construct a path between two ATMTs (namely, the distance between two ATMTs) can be decreased to as small as 2 or less. Third, when paths are routed among the entire ATMTs, the number of path multiplexes at each link can be decreased to as small as 4 or less. Fourth, the termination ratio can be kept as many as 64% or more. The termination ratio is a ratio of paths which are terminated by a particular ATMT in all paths which flows therein. The lower the termination ratio, the more the number of relays of a cell between two ATMTs. Thus, the switching resources are used with many losses. Fifth, the number of ATMTs can be easily increased and decreased. Sixth, a transmission path with the standard interface transmission rate of 155 Mb/s or 622 Mb/s can be used among the ATMTs and thereby the cost reduction is expectable. Seventh, since the ATMTs are redundantly connected, a trouble over a particular transmission path or in an ATMT does not affect the entire system without countermeasures such as switching of homing side. Eighth, since the flexibility of designs with respect to the link connection shape between the ATMTs, the link band (the number of ports assigned), and so forth is high, the user's needs can be satisfied with high flexibility.

What is claimed is:

1. A broadband switching network for transmitting information by using a cell having an information field and a header, said network comprising:

a plurality of first networks, each having a plurality of access nodes for multiplexing and demultiplexing said cell and having a ring shape transmission path for connecting said plurality of access nodes in a ring shape so as to transmit said cell; and

a second network having a plurality of switches and a separate interface connected to one of said access nodes in each one of said plurality of first networks, for relaying and switching said cell; and

transmission paths for connection to said switches so as to transmit said cell.

2. The broadband switching network as set forth in claim 1, wherein said ring shape transmission path comprises two transmission paths in one direction.

3. The broadband switching network as set forth in claim 1, wherein each said first network is arranged to autonomously operate.

4. The broadband switching network as set forth in claim 2, wherein each said first network is arranged to autonomously operate.

5. The broadband switching network as set forth in claim 1, wherein each said first network has a call process, maintenance, and management ring access node for call processing, system maintaining, and managing each said first network.

6. The broadband switching network as set forth in claim 2, wherein each said first network has a call process, maintenance, and management ring access node for call processing, system maintaining, and managing each said first network.

7. The broadband switching network as set forth in claim 3, wherein each said first network has a call process, maintenance, and management ring access node for call processing, system maintaining, and managing each said first network.

8. The broadband switching network as set forth in claim 4, wherein each said first network has a call process, maintenance, and management ring access node for call processing, system maintaining, and managing each said first network.

9. The broadband switching network as set forth in claim 1, wherein each said first network has a traffic shaping function for suppressing burstiness of the flow of said cell.

10. The broadband switching network as set forth in claim 2, wherein each said first network has a traffic shaping function for suppressing burstiness of the flow of said cell.

11. The broadband switching network as set forth in claim 3, wherein each said first network has a traffic shaping function for suppressing burstiness of the flow of said cell.

12. The broadband switching network as set forth in claim 5, wherein each said first network has a traffic shaping function for suppressing burstiness of the flow of said cell.

13. The broadband switching network as set forth in claim 1, further comprising a plurality of said second networks, at least some of said second networks having Separate interfaces connected to one of said access nodes in each said first network in different pluralities of said first networks, wherein said second networks are connected by said plurality of transmission paths in a wheel shape.

14. The broadband switching network as set forth in claim 1, further comprising a plurality of said second networks, at least some of said second networks having separate interfaces connected to one of said access nodes in each said first network in different pluralities of said first networks, wherein said second networks are connected by said plurality of transmission paths in a ring shape.

15. The broadband switching network as set forth in claim 1, further comprising a plurality of said second networks, at least some of said second networks having separate interfaces connected to one of said access nodes in each said first network in different pluralities of said first networks, wherein said second networks are connected by said transmission paths with an optical loop network having a plurality of stations and an optical loop transmission path for connecting said plurality of stations in a loop shape.

16. The broadband switching network as set forth in claim 15, wherein at least one of said plurality of stations is connected by said transmission paths to two or more of said plurality of second networks.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 5,566,179
DATED : October 15, 1996
INVENTOR(S) : Hiroshi KOBAYASHI et al.

It is certified that error appears in the above-indentified patent and that said Letters Patent is hereby corrected as shown below:

Claim 13, column 12, line 12, "Separate" should read --separate--.

Signed and Sealed this

Twenty-ninth Day of April, 1997

Attest:

BRUCE LEHMAN

Attesting Officer

Commissioner of Patents and Trademarks